The Grill: Innovation guru John Seely Brown says it's a great time to explore fresh ideas, such as internal and external cloud computing. PAGE 23

COMPUTERWORLD®

SPECIAL REPORT

BLINDSIDED!

They thought their stored data was locked tight, but they were wrong. Read about five of the biggest storage mishaps yet and how you can avoid a similar fate. PAGE 26

#BXBBJFT**********CAR-RT LOT**C-035
#1154488/CB/2# 0906 001 21 041

1542-1
NATIONAL ARCHIVE PUBLISHING 63
PO BOX 998
300 N ZEEB RD
ANN ARBOR MI 48103-1553

Inside

FEBRUARY 9, 2009
VOL. 43, NO. 6 $5/COPY

News & Analysis

Microsoft shortens the list of Windows 7 editions it will offer – sort of. PAGE 6

Spending on SaaS is growing at double-digit rates, as users look to cut software costs. PAGE 12

Despite the recession, the tech jobs outlook isn't all gloomy – just mostly so. PAGE 18

Opinions

The H-1B debate would be more constructive with less rancor. PAGE 4

Is Apple in trouble without Steve Jobs? Not really. PAGE 25

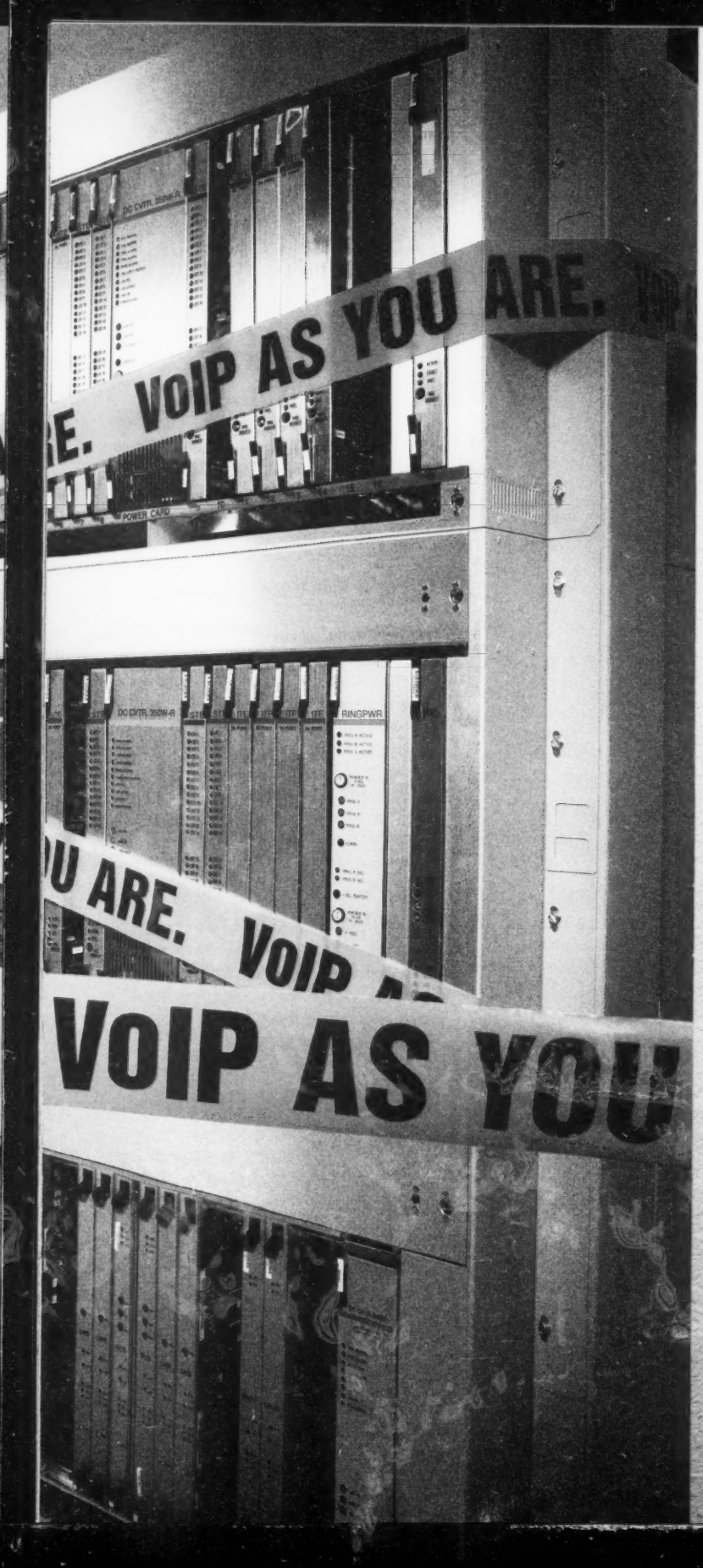
Single point of failure? In crazy times like these, it could be any one of us. PAGE 44

Careers

A list of the 10 best jobs in the country includes two from the world of IT. PAGE 40

COMPUTERWORLD.COM

VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.



Let's leave the hardware where it is.

A software-based VoIP solution from Microsoft is a whole new way to look at telephony.

As it turns out, that important move to VoIP isn't about ripping and replacing or big, upfront costs. That's because it's no longer about hardware.

It's actually about software.

That's right. Keep your hardware—your PBX, your gateways, even your phones. Add software. Software that integrates with Active Directory,® Microsoft® Office, Microsoft Exchange Server, and your PBX. Simply maximize your current PBX investment and make it part of your new software-based VoIP solution.

Because what you have is good. What you have with the right software is even better. Learn more at microsoft.com/voip

Your potential. Our passion.®

Microsoft®

Inside

COMPUTERWORLD ■ FEBRUARY 9, 2009

■ NEWS DIGEST

6 Microsoft will offer just two main versions of **Windows 7,** but six overall. | The average cost of **data breaches** to affected companies **keeps rising,** a new report says.

8 IBM is building a **20-petaflop supercomputer** for the federal government. | **SAP** launches **Business Suite 7,** a coordinated upgrade of its applications.

10 As **encryption in disk drives** spreads, users and analysts are concerned that **lost passwords** or damaged hardware could result in the **permanent loss** of critical data.

■ NEWS ANALYSIS

12 SaaS Still on the Rise, Despite Down Economy. The promise of quick savings is helping software as a service to thrive, although some users are concerned about long-term costs and security.

18 Tech Jobs Forecast: Mostly Gloomy, With Some Bright Spots. The number of IT jobs in the U.S. is shrinking in response to the economic recession, but some users and vendors are still hiring.

■ DEPARTMENTS AND OPINIONS

4 Editor's Note: **Don Tennant** laments the fact that an uncivil tone often tarnishes the H-1B debate.

25 Scot Finnie proposes that Steve Jobs' absence from Apple might not be such a bad thing.

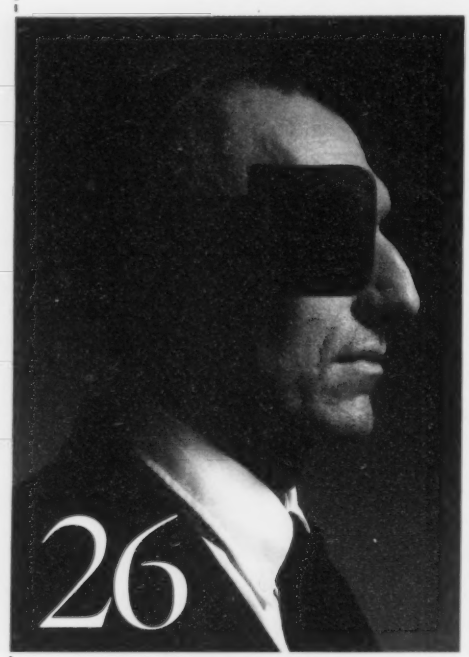
40 Career Watch: Two IT positions make it into a new ranking of the top 10 jobs in the nation.

42 Shark Tank: Boss gives pilot fish a refresher course on the policy about accepting gifts from vendors (and who has to obey it).

44 Frankly Speaking: **Frank Hayes** worries that when we're all overworked, we're all potentially single points of failure.

■ ALSO IN THIS ISSUE

Letters	5
Company Index	42

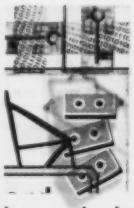


26 Blindsided!

Breaches of stored data are rising steadily, yet many companies still don't know how to protect against them. Here's a look at five headline-grabbing breaches and how you can avoid similar mishaps.

32 Locked Down in The Data Center

Storage professionals describe the latest techniques for protecting stored data within company walls.

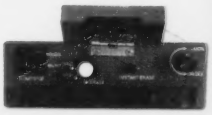


34 Locked Down in Transit

IT managers are often hampered in their efforts to protect tapes and laptops because they buy into one or more of six common myths about movable media. (Myth 1: Tapes are obsolete.)

36 Solid State's New Kill Switch

By taking advantage of a key property of the flash memory chips that make up solid-state disks, systems manufacturers are creating "fast-erase" features. Available today for military use, this functionality could catch on for business applications ranging from back-end enterprise SSD storage to executive laptops.



BitMicro's removable SSD

37 QuickStudy

Our primer on XAM, or Extensible Access Method, explains how the technology is used to preserve the authenticity of "fixed" content, such as stored e-mail and images of X-rays or cancelled checks.

38 Opinion

Without an overall game plan for storage security, it's likely that efforts will be duplicated in some areas and that tasks will be overlooked in others, says columnist James Damoulakis, CTO at GlassHouse Technologies.

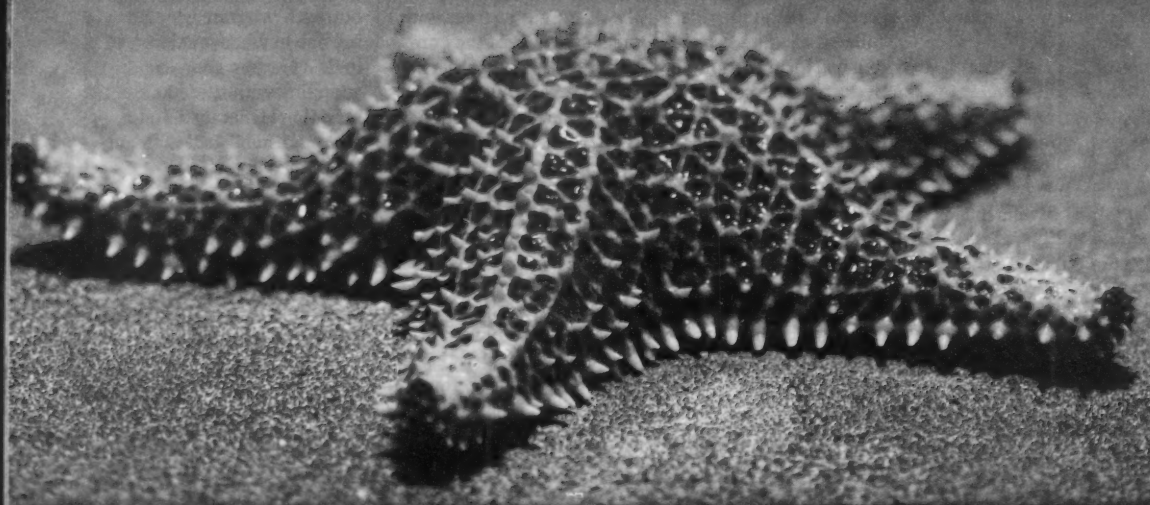
ONLINE Visit **www.computerworld.com/more** to take the Storage Networking Industry Association's **storage security self-assessment quiz** and evaluate how well your stored data is protected. Plus, brush up on storage terms with SNIA's **online glossary.**

You can also find other resources from SNIA's Storage Security Industry Forum, like storage security best practices, a guide to securing data at rest and information about a career as a storage security professional.

Starfish lack one centralized brain.

They can't process information seamlessly.
But you can. With proven business analytics software and services from SAS.

www.sas.com/starfish



SAS SOFTWARE HELPS COMPANIES ACROSS EVERY INDUSTRY DISCOVER INNOVATIVE WAYS TO INCREASE PROFITS, MANAGE RISK AND OPTIMIZE PERFORMANCE.

SAS® Business Analytics

*Visit www.sas.com/starfish for **details on our software and services***

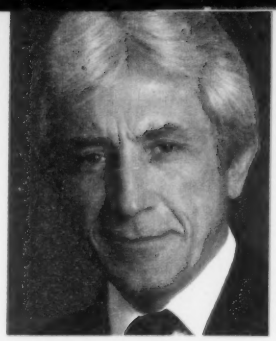
- Data integration
- Analytics
- Query and reporting
- Performance management
- Targeted business and industry solutions

sas | THE POWER TO KNOW.

■ EDITOR'S NOTE

Don Tennant

Tarnished Discourse



IF THERE'S one thing we hate doing around here, it's removing reader comments from our Web site. We feel very strongly that our readers' voices should be heard, regardless of how objectionable any one of us might find a particular viewpoint. But there are occasions when the right thing to do is pull the plug.

Such an occasion arose last Wednesday morning, when we were compelled to remove a comment that had been posted by a reader in a discussion prompted by one of my recent blog postings on the H-1B visa issue. Anyone who has read any of the comments from readers responding to our H-1B coverage knows how controversial the topic is. It's also fairly obvious that we don't censor comments that are directed at any one of us here at *Computerworld*. Journalists tend to have thick skins, so even malicious comments in that category, as long as they don't also direct hatred toward a particular group, are willingly condoned.

But it's different when the malice is directed at other readers. And when the forum degrades into a vehicle for hate speech, we make no apologies for deleting any offending post. That's what happened Wednesday, when we removed a derogatory, demeaning comment directed at a reader presumed by the poster to be from India.

The blog post that spawned that discussion was one in which I provided the full text of a newsletter written by Norm Matloff, a university professor and well-known critic of the H-1B program. Matloff had devoted the entire newsletter to rebutting last week's Editor's Note, in which I contended that the blame being directed at foreign workers and those who hire them is misplaced.

As I wrote in that blog posting, my goal has simply been to advance the H-1B discussion, and no one has advanced it more admirably than Matloff. That he contested the views I expressed is beside the point. It makes absolutely no difference to me — nor should it — whether a contributor to the discussion agrees with me. The value of the contribution lies in furthering informed discourse on the issue. That the discourse is so frequently tarnished by mean-spirited attacks — and, occasionally, by hate speech — is a shame. Imagine how much more constructive the H-1B debate would be if it were conducted in a manner in which opposing viewpoints were appreciated and respected.

■ When the forum degrades into a vehicle for hate speech, we make no apologies for deleting any offending post.

It's not as hard to imagine as you might think. Coincidentally enough, it was also on Wednesday morning that I received an e-mail from an IT manager in Connecticut who wrote that he had to "admit it took every ounce of self control not to send harsh feedback or post a comment that was full of bile." Instead, he went on to write a reasoned, engaging response in which he explained why he felt that the H-1B program should be discontinued. As I told him in my reply, I couldn't have asked for input that was more exemplary in promoting thoughtful discourse.

Nor is it difficult to imagine ways in which such discourse can be advanced. A couple of weeks ago, I spoke with some people from New York who are working with enterprise systems management software vendor CA to enrich the education of students in the city's school system. CA has focused its philanthropy on education, and it's participating in a number of outreach programs, including one in which students in East Harlem are corresponding with students at a school in Hyderabad, India, that CA established with the Hope Foundation.

"Now they can talk to each other about what their lives are like, hopefully just expanding their horizons and giving them new ways to explore and learn," said Anne Marie Agnelli, CA's vice president of North American communications and community affairs.

Yeah, they can. And it's gratifying to imagine how far their exploration will take them from what tarnishes our discourse today. ■

Don Tennant *is* Computerworld's *senior editor-at-large. You can contact him at don_tennant@computerworld.com, and visit his blog at* http://blogs.computerworld.com/tennant.

Not the Time to Regress In IT Management

I often enjoy reading the topics Don Tennant tackles in his Editor's Note and usually can relate on a professional level. With the Jan. 19 column, "The Other Casualty," I could relate on an academic level, since I'm currently enrolled in the Managing Information Technology master's program of the Robinson School of Business at Georgia State University.

I share Tennant's concern regarding the loss of knowledge-sharing opportunities such as the discarded MSIT-ITSM program at Carnegie Mellon University. My 12 years in IT have been predominantly in the areas of software engineering and application architecture, and I wanted to move toward managing IT with a holistic approach instead of the typical silo mentality. The past six months have opened my eyes to the need for IT management that can move forward in tackling challenges that normally cause IT to retrogress.

■ **David A. Tatum Jr.,** *solutions manager, Fiserv Inc., Atlanta, david.tatum@fiserv.com*

Cost Concerns Usually Drive IT Change Efforts

I greatly enjoyed Gary Anthes' column "Out With the Old, In With the New" in the Jan. 19 issue of *Computerworld*. I am now going to spoil my compliment with my input (this proves I am a programmer at heart).

Anthes said that an IT manager's main motivation for changing processes, procedures and tools is "that he needs a better idea in order to deflect criticism for that downtime last week and to justify a budget increase." But I have found it's usually cost-reduction requirements that drive such changes.

Still, Anthes is correct that many of the changes attempted by IT managers fail and that "changing . . . is much more expensive and painful than anyone expected, and not all the promised benefits are realized."

When a change fails, the IT manager is forced to hide the failure and sell the effort as a success to those he reports to. Few, if any, IT managers will admit that they wasted money and resources because they didn't understand the change effort.

■ **Tim Magee,** *Lexington, Ky., tmagee@ureach.com*

COMPUTERWORLD.COM

Find these stories at computerworld.com/more

5 Mobile Tech 2010: Five Major Trends

The next two years will bring a slew of advances for mobile workers. Here are five that could make life on the road more productive.

Will the App Store Change The Software Market?

OPINION: Apple's App Store worked for the iPhone, so maybe this new software-distribution model could work for all kinds of devices, including desktops, says Ryan Faas.

$ IT Layoff Tracker

Check out *Computerworld*'s interactive database of announced staff cuts at tech companies.

Who Owns the Code?

Unless you plan ahead and take some time to brush up on copyright laws, collaborations with outside developers can muddy the legal waters in all sorts of ways.

A Look at Three NAS Devices

REVIEW: If your storage needs are heading into terabyte territory, you might want to check out network-attached storage options. We examine three products that offer big-time storage for small networks.

MaxNAS RAID ▶ with iSCSI

COMPUTERWORLD

P.O. Box 9171, 1 Speen Street
Framingham, MA 01701
(508) 879-0700
Computerworld.com

■ **EDITORIAL**

Editor in Chief Scot Finnie

Senior Editor-at-Large Don Tennant

Executive Editors Mitch Betts, Julia King (events)

Managing Editors Michele Lee DeFilippo (production), Sharon Machlis (online), Ken Mingis (news)

Design Director Stephanie Faucher

Director of Blogs Joyce Carpenter

Technologies Editor Johanna Ambrosio

Features Editors Kathleen Melymuka, Valerie Potter, Ellen Fanning (special reports), Barbara Krasnoff (reviews)

Senior Editor Mike Barton (new media)

Senior News Editor Craig Stedman

News Editors Mike Bucken, Marian Prokop

National Correspondents Gary Anthes, Julia King, Robert L. Mitchell

Reporters Sharon Gaudin, Matt Hamblen, Gregg Keizer, Eric Lai, Lucas Mearian, Patrick Thibodeau, Jaikumar Vijayan

Features Writer, Video Editor David Ramel

Assistant Managing Editor Bob Rawson (production)

Senior News Columnist Frank Hayes

Art Director April Montgomery

Research Manager Mari Keefe

Senior Copy Editors Eugene Demaitre, Monica Sambataro

Copy Editor Donna Sussman

Associate Editor, Community Ken Gagné

Office Manager Linda Gorgone

Contributing Editors Jamie Eckle, Preston Gralla, Tracy Mayor

■ **CONTACTS**

Phone numbers, e-mail addresses and reporters' beats are available online at *Computerworld.com* (see Contacts link at the bottom of the home page).

Letters to the Editor Send to letters@computerworld.com. Include an address and phone number for immediate verification. Letters will be edited for brevity and clarity.

News tips newstips@computerworld.com

Subscriptions and back issues (888) 559-7327, cw@omeda.com

Reprints/permissions The YGS Group, (800) 290-5460, ext. 148, computerworld@theygsgroup.com

News Digest

FIND THE FULL STORIES AT
COMPUTERWORLD.COM

THE WEEK AHEAD

TUESDAY: Microsoft plans to issue four security fixes, two of them rated "critical," in its monthly software patch release.

TUESDAY: AMD is due to hold a stockholders meeting in Austin on the planned spin-off of its chip plants.

WEDNESDAY: A pretrial hearing is scheduled in San Francisco Superior Court in the case of Terry Childs, the network administrator charged with locking up the city's WAN last year. (See related items, pages 8 and 44.)

<< A screenshot from the Windows 7 beta release

OPERATING SYSTEMS

Windows 7: Two Main Editions, Six All Told

LOOKING TO address complaints about the proliferation of Windows editions, Microsoft Corp. last week said it will sell Windows 7 in two primary versions: one for business users and the other for consumers.

However, the software vendor will still offer six editions of the upcoming operating system altogether. Mike Ybarra, Microsoft's Windows general manager, said the various versions are necessary in order to fully meet the needs of PC makers and the huge base of Windows users.

"We did a lot of research and talked to a lot of [hardware] partners and customers," Ybarra said. "Our biggest challenge is that we have over 1 billion customers. It's hard to satisfy all of them [with two versions]."

Windows 7 Professional will be the principal version for businesses, with a Home Premium edition as its peer on the consumer side. That hearkens back to Microsoft's licensing strategy for Windows XP, which similarly had two main editions.

But like its predecessor, Windows Vista, Windows 7 will also be available in an Enterprise edition for large corporate customers with volume licensing agreements. That version will include advanced networking and security features that won't be in the Professional edition, Microsoft said.

An Ultimate edition with the same feature set as the Enterprise one may appeal to businesses that don't want to lock themselves into a multiyear licensing deal, said Matt Rosoff, an analyst at Directions on Microsoft in Kirkland, Wash. But Rosoff thinks the Windows lineup remains too complicated for business users.

Ybarra said Microsoft considered cutting the Ultimate edition, aimed mainly at gamers and PC enthusiasts. But PC vendors wanted that version to be kept because they see it as a way to differentiate their systems.

Separately, Microsoft said it will offer upgrades from the seven-year-old XP to Windows 7. But that simply means users will be able to buy discounted upgrade licenses; XP machines would require clean installations of Windows 7, meaning their hard drives would be overwritten.

— Eric Lai, with Gregg Keizer

SECURITY

Data Breaches Continue to Get More Costly

THE AVERAGE COST of data breaches to the companies hit by them continues to increase, according to a report by the Ponemon Institute.

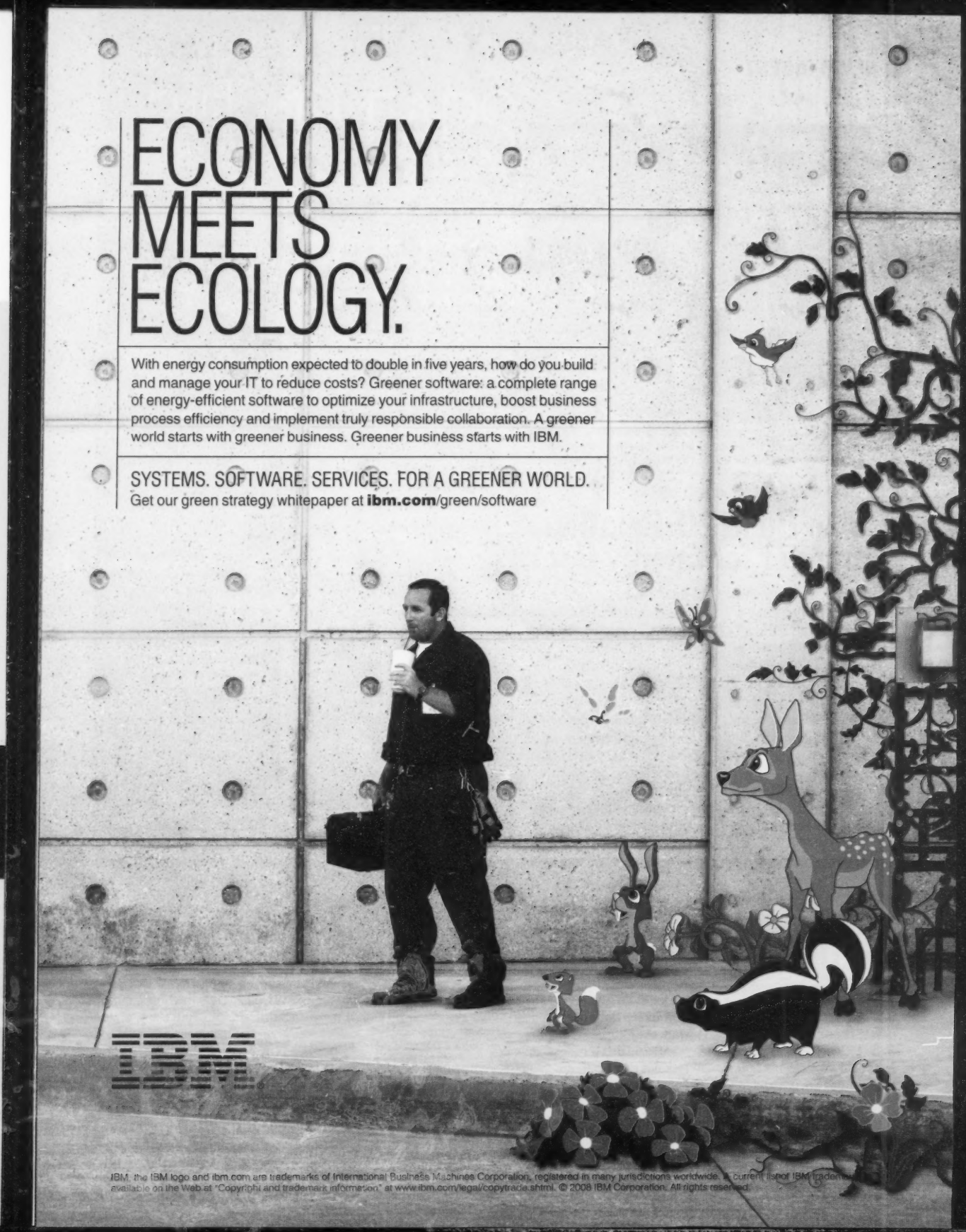
The study of 43 breaches disclosed last year found that costs averaged $202 per compromised customer record – up from $197 in 2007 and $182 in 2006. Overall costs ranged from $613,000 to $32 million, with the number of compromised records ranging from about 4,200 to 113,000.

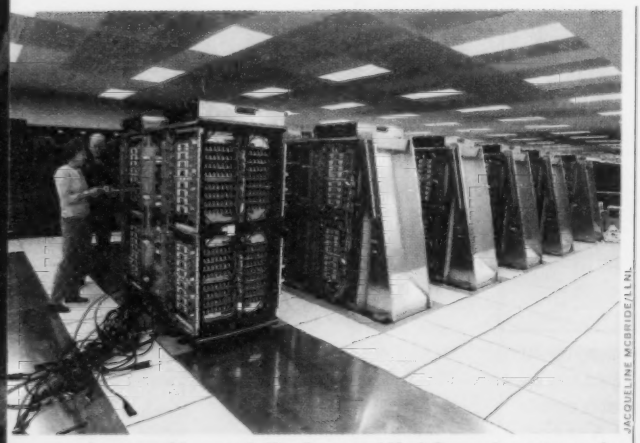
Ponemon's figures include direct expenses for breach detection, mitigation and response, plus indirect costs like customer defections.

Increasingly, the biggest cost to companies is lost business, which accounted for $139 of the average breach cost, said Larry Ponemon, the think tank's chairman.

Gartner Inc. analyst John Pescatore said Ponemon's figures were "in the ballpark" of Gartner's own cost estimates for breaches involving up to 100,000 records. "It's a little lower than what we've seen" – but not by much, he said.

– JAIKUMAR VIJAYAN


ECONOMY
MEETS
ECOLOGY.
With energy consumption expected to double in five years, how do you build and manage your IT to reduce costs? Greener software: a complete range of energy-efficient software to optimize your infrastructure, boost business process efficiency and implement truly responsible collaboration. A greener world starts with greener business. Greener business starts with IBM.
SYSTEMS. SOFTWARE. SERVICES. FOR A GREENER WORLD.
Get our green strategy whitepaper at ibm.com/green/software
IBM
IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml. © 2008 IBM Corporation. All rights reserved.



JACQUELINE MCBRIDE/LLNL

Lawrence Livermore's Kim Cupps and Mark Seager inspect a newly installed rack for Dawn, a 500-teraflop IBM BlueGene/P system. Dawn will help lay the foundation for the 20-petaflop Sequoia.

HIGH-PERFORMANCE COMPUTING

IBM to Build 20-Petaflop Computer for Energy Dept.

THE U.S. government has awarded IBM a contract to build a supercomputer capable of performing at 20 petaflops, which is more powerful than all of the systems on today's Top500 supercomputer list combined.

Terms of the deal were not disclosed.

Nuclear researchers at the U.S. Department of Energy will use the planned Sequoia system, to be built in IBM's plant in Rochester, Minn.

The fastest systems today perform at a little over 1 petaflop, or 1 thousand trillion floating-point operations per second. The single-petaflop barrier was passed last May by IBM's Roadrunner supercomputer.

Sequoia will be housed at the Lawrence Livermore National Laboratory. Mark Seager, assistant department head for advanced technology at Lawrence Livermore, called the new system "the biggest leap of computing capability ever delivered to the lab."

The Linux-based Sequoia system will use approximately 1.6 million IBM Power processors. IBM is still developing a 45-nanometer chip for the system and may produce a processor with eight, 16 or more cores. The system will have 1.6TB of memory and will be housed in 96 refrigerator-size racks.

The Sequoia contract also calls for IBM to deliver a smaller, 500-teraflop system, called Dawn, to the Livermore, Calif.-based lab. Dawn will be operational later this year, and researchers will use it to prepare for the larger system.

The national lab's work with Sequoia will likely pave the way for broader adoption of massive systems that could improve weather research, forecasts, tornado tracking and work on a variety of other research problems, officials said.

— Patrick Thibodeau

Short Takes

Intel Corp. has delayed the release of the quad-core Tukwila chip, its next-generation 64-bit Itanium processor. The company needs time to add new memory technology to improve server performance and to add backward-compatibility for future chips.

Terry Childs, a former San Francisco city network administrator who was jailed last summer for allegedly holding the city's network hostage, is seeking $3 million from the city for what he claimed was a wrongful arrest.

Oracle Corp. has issued 102 subpoenas to 99 former customers of TomorrowNow, the now-shuttered SAP subsidiary at the heart of Oracle's lawsuit against SAP AG. The lawsuit alleges that TomorrowNow employees illegally downloaded Oracle material.

Mozilla Corp. released an updated version of the Firefox browser. It said the new release fixes bugs that hackers could exploit to run unauthorized software on a PC.

ENTERPRISE APPLICATIONS

SAP Unveils Full Upgrade Of ERP Suite

SAP AG last week unveiled a new version of its Business Suite ERP software, which analysts said marks the first time the modules are integrated on a single underlying platform.

"People have had this perception that it's this one integrated system, but the reality is the [systems integrators] have been tying all these [modules] together, making them work," said Ray Wang, an analyst at Forrester Research Inc. Now the full suite sits atop SAP's SOA-based NetWeaver middleware platform.

SAP said that Business Suite 7 includes more than 150 "functional innovations" and expands on the company's "enhancement package" strategy, which allows users to add specific functions without a full upgrade.

SAP ROJOE WALLACE

At a launch event in New York, SAP officials said Business Suite 7 features more than 150 "functional innovations."

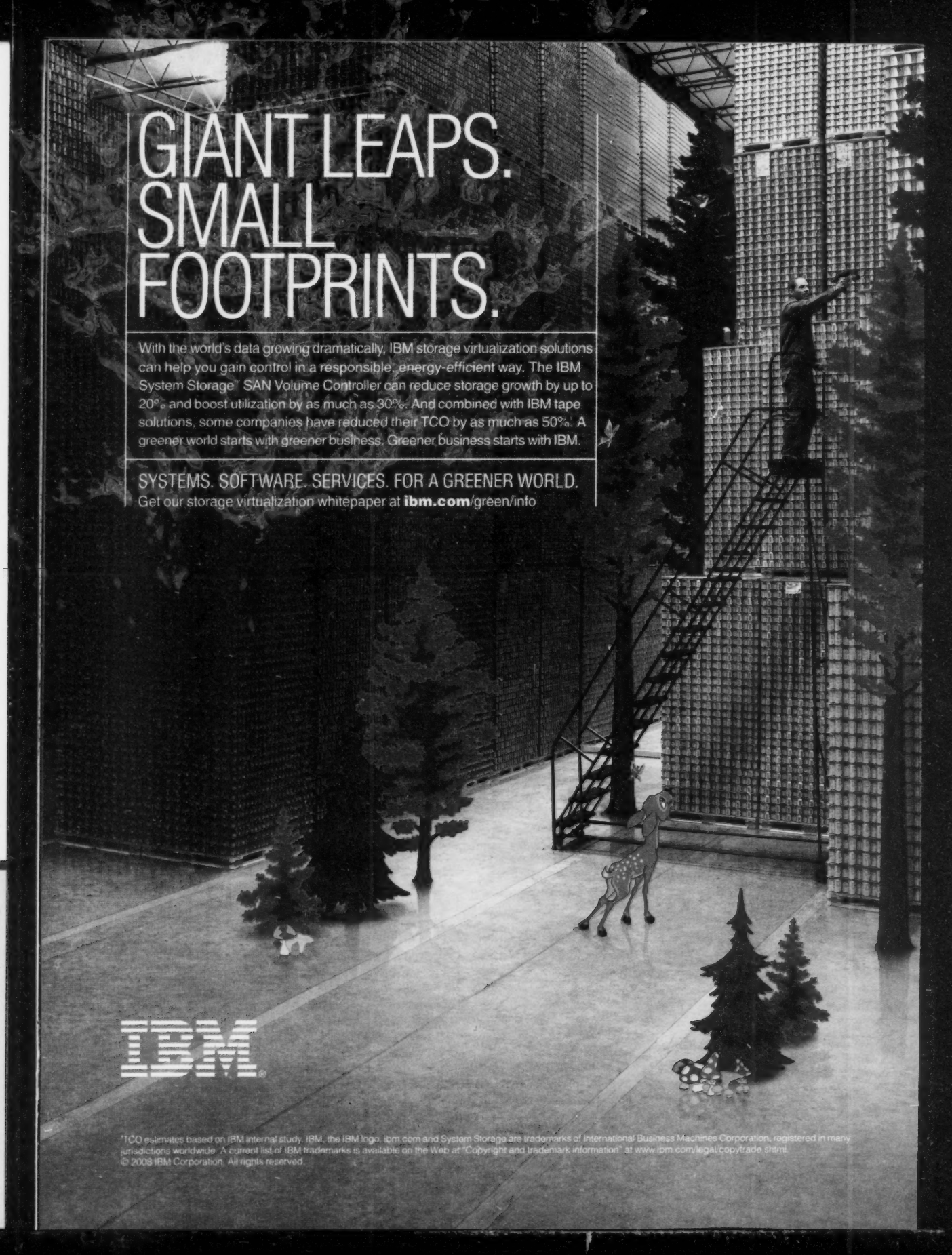
A spokesman added that the upgraded suite also includes a dashboard-like interface to pull in relevant information from different modules.

At a launch event in New York, SAP CEO Leo Apotheker called the new offering "a keystone we will build on for the future."

Jennifer Allerton, CIO at Roche Holding Ltd.'s pharmaceutical division, said SAP's new synchronized release schedule is good for her company.

In the past, release dates for individual modules were "all over the place," she said. "Now it's easier to plan for them."

CHRIS KANARACUS, IDG NEWS SERVICE


GIANT LEAPS.
SMALL
FOOTPRINTS.
With the world's data growing dramatically, IBM storage virtualization solutions can help you gain control in a responsible, energy-efficient way. The IBM System Storage™ SAN Volume Controller can reduce storage growth by up to 20%* and boost utilization by as much as 30%*. And combined with IBM tape solutions, some companies have reduced their TCO by as much as 50%*. A greener world starts with greener business. Greener business starts with IBM.
SYSTEMS. SOFTWARE. SERVICES. FOR A GREENER WORLD.
Get our storage virtualization whitepaper at ibm.com/green/info
IBM
*TCO estimates based on IBM internal study. IBM, the IBM logo, ibm.com and System Storage are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.
© 2008 IBM Corporation. All rights reserved.

DATA STORAGE

Firms Take Steps to Head Off Encryption Dangers

THE GROWING call to encrypt stored data is raising questions among users and analysts fearful that a lost password or damaged drive could bury important information forever.

Some industry observers believe that a new Trusted Computing Group (TCG) standard, released last month, could lead all hard disk and solid-state drive makers to add encryption capabilities to most products within five years. Most of the top storage vendors are members of the TCG.

> **"[Encrypting data] is still a million times better than having nothing.**
> KEN WARING, IT DIRECTOR, CBI HEALTH

Corporate IT managers acknowledge the potential problems but say that steps can be taken to overcome them. For example, AdaptaSoft Inc., a maker of payroll systems software, requires workers to store critical data on the company's network drive rather than on laptops with encrypted hard disk drives, said CIO David Virkler.

AdaptaSoft installed Seagate's self-encrypting, 2.5-in. Momentus 5400.2 drives on its Dell laptops in October 2007 to better protect customers' financial data. Virkler also noted that implementing a group policy eased what could have been a "painful" rollout of the drives.

Ken Waring, IT director at Toronto-based CBI Health, said that despite the potential for problems, encrypting data "is still a million times better than having nothing." The company, which operates 135 health care facilities throughout Canada, must do all it can to protect sensitive patient information, he said.

Today, 90 of CBI Health's 200 laptops use Seagate Momentus drives with native full-disk encryption, and the rest will be on a regular product-upgrade schedule.

Dave Hill, an analyst at Mesabi Group, said that well-managed, full-disk encryption ensures that lost or stolen data can't be accessed and that companies are in compliance with most state data-breach notification laws.

— Lucas Mearian

BETWEEN THE LINES *By John Klossner*

BENCHMARKS LAST WEEK

William Amelio resigned as CEO of Lenovo Group Ltd. after a $97 million Q3 loss. Lenovo replaced him with an executive in China and said it plans to focus more on the PC market there.

Michael Widenius, MySQL's original developer, resigned from database owner Sun Microsystems Inc. Marten Mickos, head of Sun's database unit and MySQL AB's former CEO, is also leaving.

NINE YEARS AGO: Ford Motor Co. and Delta Air Lines Inc. announced plans to offer all employees home computers and Internet access for small monthly fees.

Global Dispatches

Satyam Promotes Murty to CEO

HYDERABAD, India – Struggling Satyam Computer Services Ltd. last week promoted 15-year company veteran A.S. Murty to CEO, a move that may be temporary as the company looks to sell itself.

The company also said that it has raised about $130 million (U.S.) in working capital from banks as advisers – The Boston Consulting Group, Goldman Sachs and Avendus Capital – evaluate its strategic options. Some companies, including outsourcers HCL Technologies Ltd. and iGate Corp., have shown interest in investing in Satyam.

The firm plunged into a financial crisis last month after its founder and former chairman, B. Ramalinga Raju, admitted that Satyam had inflated its financial results for several years. Raju and two other top executives resigned at the time.

John Ribeiro,
IDG News Service

Intel Shuttering Chinese Plant To Cut Costs

SHANGHAI – Intel Corp. last week announced that it is closing a chip testing and assembly plant here as part of a restructuring of its Chinese operations that is designed to cut costs.

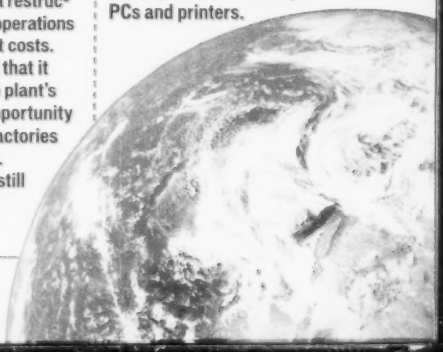
The company said that it will offer some of the plant's 2,000 workers an opportunity to take jobs at Intel factories in Chengdu or Dalian.

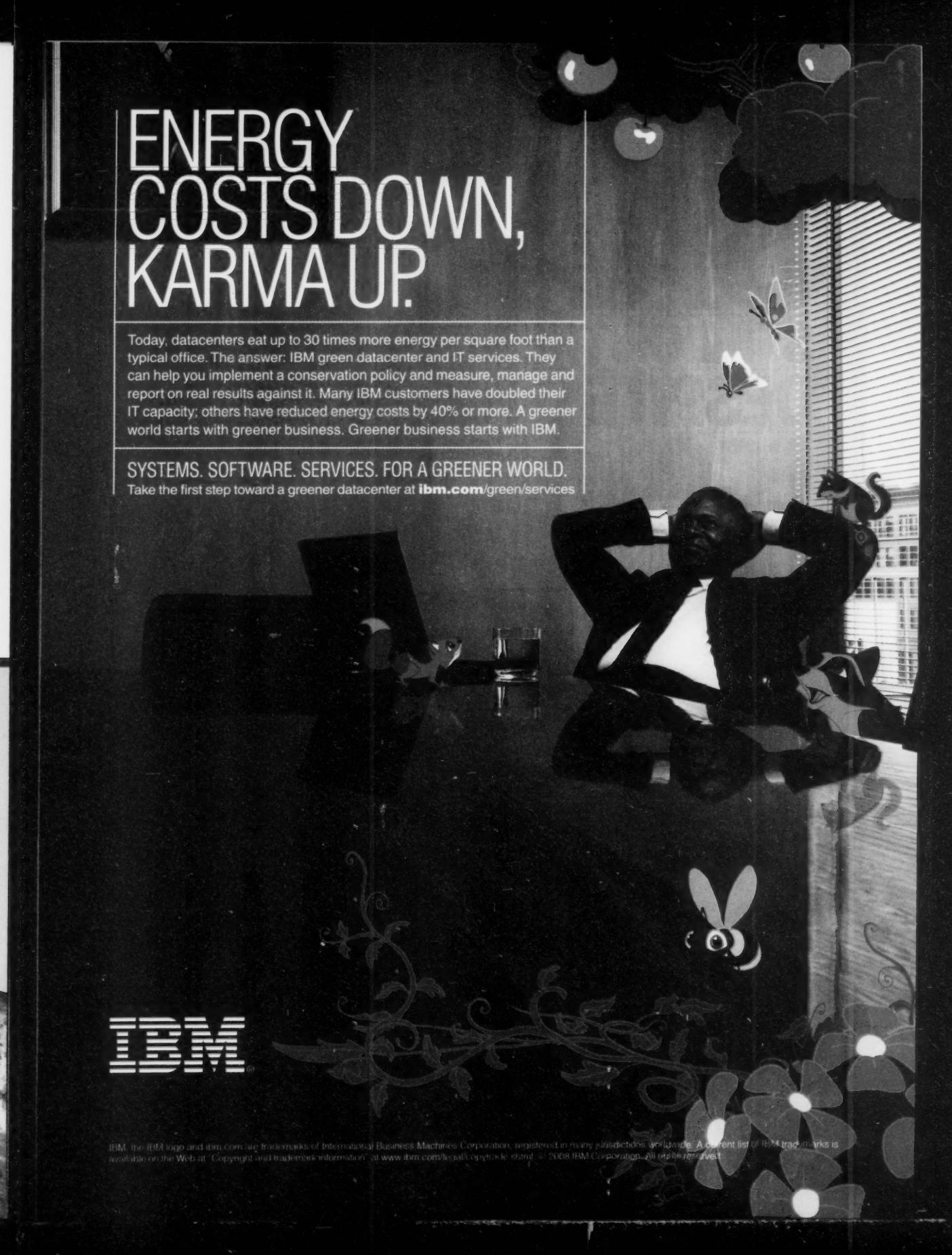
Intel added that it still plans to build a new 300-millimeter chip factory in Dalian and maintain its R&D operations in Shanghai.

Dan Nystedt,
IDG News Service

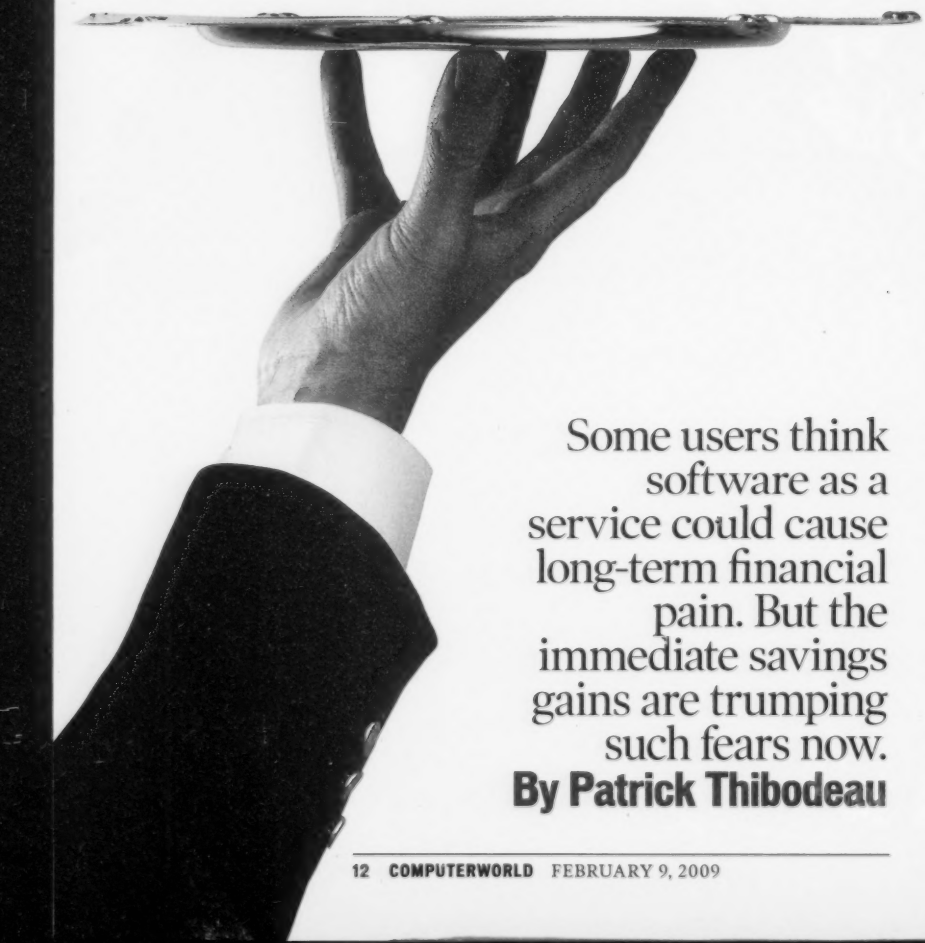
BRIEFLY NOTED

The Bavarian State Ministry of Justice and Consumer Protection has awarded a three-year contract to Unisys Corp.'s subsidiary in Sulzbach, Germany, to continue managing the agency's IT infrastructure. Terms weren't disclosed. Unisys will also install storage virtualization technologies and replace the ministry's PCs and printers.




ENERGY
COSTS DOWN,
KARMA UP.
Today, datacenters eat up to 30 times more energy per square foot than a typical office. The answer: IBM green datacenter and IT services. They can help you implement a conservation policy and measure, manage and report on real results against it. Many IBM customers have doubled their IT capacity; others have reduced energy costs by 40% or more. A greener world starts with greener business. Greener business starts with IBM.
SYSTEMS. SOFTWARE. SERVICES. FOR A GREENER WORLD.
Take the first step toward a greener datacenter at ibm.com/green/services
IBM
IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml. © 2008 IBM Corporation. All rights reserved.

SAAS STILL ON THE RISE, DESPITE DOWN ECONOMY



© FOTOLIA / GUILLERMO LOBO

Some users think software as a service could cause long-term financial pain. But the immediate savings gains are trumping such fears now.

By Patrick Thibodeau

OVERALL IT spending has slowed down, forcing many IT vendors to lay off workers. But spending on software-as-a-service applications is growing at double-digit rates, as users look to take advantage of the relatively low cost of implementing SaaS technologies.

To be sure, SaaS is still very much a niche market from the standpoint of both revenue and user adoption levels. For instance, market research firm IDC expects $12.4 billion in SaaS spending worldwide this year — a drop in the bucket of the overall IT market.

But two weeks ago, IDC raised its projected SaaS growth rate for 2009 from 36% to 40.5%. The firm said recent surveys indicated that the recession would prompt more users to choose subscription-based services over on-premises applications. IDC also forecast that nearly 45% of U.S. companies will spend at least one-fourth of their IT budgets on SaaS by next year, up from 23% in 2008.

"I think SaaS has an element of being recession-proof," said Forrester Research Inc. analyst Ray Wang. Forrester last month released a report on the subscription revenue growth rates at Salesforce.com Inc. and nine other SaaS vendors; most reported year-to-year gains of more than 40% in the third quarter of 2008.

Wang did offer some caveats about the SaaS market, noting that many corporate users are proceeding cautiously, with small deployments and short contracts — even month-to-month agreements. "People are likely to be commitment-phobic," Wang said.

More often than not,

Continued on page 16

Work with InterSystems.

Not separate systems.

Partners Healthcare works with InterSystems.

The IT group at Partners Healthcare System in New England is an innovator in connected healthcare. They work with InterSystems **Ensemble®** software to deliver better care at lower costs to over four million patients.

Ensemble is a rapid integration and development platform that makes it much easier to connect applications, processes, and people – and to develop composite applications.

Ensemble includes InterSystems **Caché®**, the world's fastest object database. Caché's lightning speed, massive scalability, and rapid development environment give Ensemble unmatched capabilities.

For 30 years, we've been a creative technology partner for leading enterprises that rely on the high performance of our products. Ensemble and Caché are so reliable that the world's best hospitals use them for life-or-death systems.

INTERSYSTEMS

Read the case study about Partners Healthcare at **InterSystems.com/Connect18A**

© 2009 InterSystems Corporation. All rights reserved. InterSystems Ensemble and InterSystems Caché are registered trademarks of InterSystems Corporation.
© Copyright 2008 Partners HealthCare System, Inc. Other product names are the trademarks of their respective vendors.2-09 Work18CoWo

Can your backup software *do this*?

- Eliminate up to half your tape drives
- Eliminate the backup window
- Deduplicate enterprise data across all tiers, including tape
- Reclaim space on primary storage
- Archive, preserve, and search information for eDiscovery
- Reduce off-site tapes by up to 90%
- Reduce data management costs by up to 40%

CommVault Corporate Headquarters 2 Crescent Place Oceanport, NJ 07757

Individual cost savings and performance improvements may vary.

©1999-2009 CommVault Systems, Inc. All rights reserved. CommVault, the "CV" logo, Solving Forward, and Simpana are trademarks or registered trademarks of CommVault Systems, Inc. All other third party brands, products, service names, trademarks, or registered service marks are the property of and used to identify the products or services of their respective owners. All specifications are subject to change without notice.

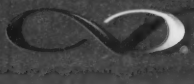
introducing

SIMPANA 8®

Leading companies worldwide are flocking to CommVault and its #1 end-user-ranked enterprise backup product. But backup is just the beginning. With the industry's only truly unified single platform, Simpana® software provides a dramatically superior way for enterprises to handle data protection, eDiscovery, recovery, and information management requirements.

Now, the groundbreaking new features of Simpana 8 make it easier than ever to solve immediate backup and data management problems, improve operations, lower costs, eliminate disparate point products, and set your enterprise up with a scalable platform to meet your needs far into the future.

Sound too good to be true? We'll be happy to prove it to you. Call 888-667-2451. Or visit **www.commvault.com/simpana** to sign up for an introductory webinar.



commvault®

solving forward®

BACKUP & RECOVERY ► ARCHIVE ► REPLICATION ► RESOURCE MANAGEMENT ► SEARCH

SAAS FUTURES

- Market researcher IDC predicts that by the end of this year, 76% of U.S. companies will be using at least one SaaS application.
- Also by year's end, nearly 35% of worldwide SaaS revenue will come from outside the U.S., IDC says.
- Almost 90% of 258 organizations that responded to a Gartner Inc. survey last summer said they planned to increase or maintain their use of SaaS technologies.

Continued from page 12

users aren't certain whether it would actually cost less to use a SaaS application than run an in-house one because they don't have a good breakdown of the IT costs associated with supporting individual apps. In addition, developing precise cost comparisons can be difficult because the potential savings from SaaS implementations often involve intangible items.

For example, when companies move to SaaS, they often shift control of applications to the business units that use them. A business unit may claim that it will get a time savings if it can deal directly with a software vendor instead of having to go through the IT department. But it isn't easy to quantify such savings.

In addition, there's the question of whether SaaS users are trading off the short-term benefits of no longer having to run applications internally in return for some potential long-term financial pain, in the form of ongoing subscription fees.

Despite such issues, SaaS technologies are now being adopted by some very large organizations, including the U.S. Army and Sonoco Products Co., a $4 billion maker of packaging products in Hartsville, S.C.

Jennifer Roberts, Sonoco's supply systems manager, said she was able make an apples-to-apples cost comparison of SaaS vs. in-house software. And in Sonoco's case, she thinks the SaaS approach will cost less.

Sonoco is a longtime user of the on-premises version of Ariba Inc.'s procurement applications. But the company wanted to expand its use of the software, and Roberts said that installing another module in-house would have required new hardware and the likely addition of an IT worker to manage and monitor the system.

That would have pushed Sonoco's long-term costs above what it's paying Ariba for the SaaS deployment, according to Roberts, who declined to disclose specific cost information.

Roberts also predicted that SaaS will increase her leverage with vendors such as Ariba by making it easier for Sonoco to switch to rival offerings if it decides that a change is needed. "When you're dissatisfied with a tool when it's in-house, the cost of switching is much higher than if it is software as a service," she said.

The Army last fall began using Salesforce.com's hosted CRM software as part of a pilot program aimed at modernizing the military branch's recruiting efforts.

The program is centered around a facility in Philadelphia, called the Army Experience Center, that lets potential volunteers learn about military technology, explore career options, run battle simulators, play computer games and even sample military cooking. The Army collects basic contact and demographic information from visitors who register at the center, and it then uses the data to customize its recruiting pitches.

The data goes into the SaaS application, which has been integrated with an in-house system for processing recruits. That work was done for the Army by systems integrator Acumen Solutions Inc. in Vienna, Va.

"This is a new model for the government to be using SaaS in this way," said Maj. Larry Dillard, a marketing officer who is heading the Army Experience Center program. Dillard emphasized that it is still very much a pilot project, but he sees potential in SaaS.

> **"The benefits we got [from SaaS] far exceeded the cost, if you look at it from a soft-dollar standpoint.**
>
> **DEBORAH KNIGHTON,** VICE PRESIDENT OF HUMAN RESOURCES, MANE USA INC.

"In about four months, we were able to take an off-the-shelf solution, configure it and deploy it," Dillard said. That, he added, has given the Army "a very robust and very capable system for almost inconsequential cost and almost no [staff] time."

The Army is sensitive to IT security issues, for obvious reasons, and SaaS forces organizations to consider whether they want to store data on third-party systems. Dillard said the Army addressed the security issues to its satisfaction by limiting the amount of data it stores about potential recruits. No Social Security numbers or other personally identifiable information is ever entered into the Salesforce.com application, according to Dillard.

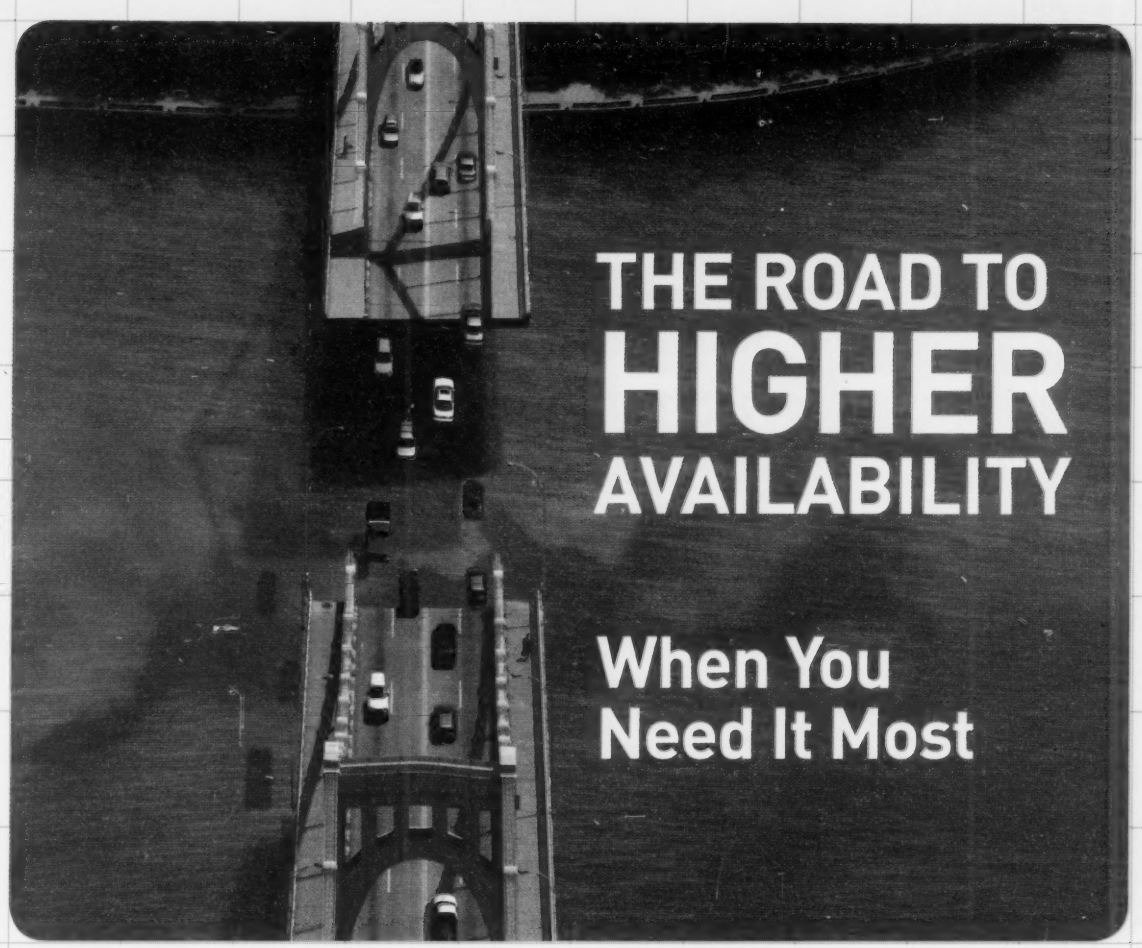
Mane USA Inc., a fragrance and flavorings maker in Wayne, N.J., adopted a SaaS version of Automatic Data Processing Inc.'s payroll and benefits software about a year ago. Employees now have self-service capabilities for making benefits changes, freeing up Mane's human resources staff to do other work, said Deborah Knighton, the company's vice president of HR.

The SaaS system has also reduced the amount of work HR needs to do to process year-end tax data, shortening the time required from several weeks to a day. "The benefits we got far exceeded the cost, if you look at it from a soft-dollar standpoint," Knighton said.

Also last year, Springs Valley Bank & Trust Co. in Jasper, Ind., switched from an in-house payroll system to SaaS software offered jointly by application developer Unicorn HRO Inc. and development tools vendor Progress Software Corp.

Craig Buse, Springs Valley's IT manager, said the in-house system was nearing the end of its life and wasn't considered to be core to the bank's business operations. With the SaaS system, Buse doesn't have to worry about updating the software or dealing with hardware failures.

But he does think that SaaS may prove to be more costly than in-house applications over time. "In general," Buse said, "you're probably going to see a little bit of a cost increase because [SaaS vendors] are doing a little more for you." ■



SunGard Availability Services help your business move forward with the most advanced and widest choice of information availability options in the industry

From virtualization to hot sites to replication and vaulting—SunGard Availability Services does it all. And it's all we do. That kind of focus helps ensure high availability of data, applications and systems and fits your needs and budget precisely.

When we partner with you, you worry less about the road ahead. Here's why: a track record of 100% successful recoveries; over 60 facilities with redundant power connected to SunGard's secure global network; and more than 20,000 end-user positions in facilities across North America and Europe. SunGard Availability Services—the information availability solution for businesses that must run non-stop.

Keep moving, call 1-800-468-7483 or visit www.availability.sungard.com.

SUNGARD® Availability Services | Keeping **People** and **Information** *Connected.®*

© FOTOLIA / MWEST

TECH JOBS FORECAST:

Mostly Gloomy, With Some Bright Spots

The number of IT positions is shrinking because of the recession. But there are still jobs to be had. **By Patrick Thibodeau**

SHORTLY AFTER Donnie Reynolds, chief operating officer at Automated HealthCare Solutions Inc. in Miramar, Fla., learned that Microsoft Corp. planned to cut 5,000 workers over the next 18 months, he and a coworker flew to the software vendor's home city of Redmond, Wash.

"We don't like to pass on a good talent," said Reynolds, who described the Jan. 26 trip to Redmond as a bit of "gonzo recruiting." He and his colleague spent part of the day outside of Microsoft's headquarters, holding banners in an effort to attract the attention of the employees there.

AHCS has also set up a new Web site aimed at Microsoft workers, featuring a picture of a beach with the tagline "This is our Vista." The site plays a song specifically chosen to appeal to people from the Seattle area: "Sunny," which begins with the line "Sunny, yesterday my life was filled with rain."

Reynolds said the medical services provider now has more than 100 résumés, some of them from Microsoft employees, for about a dozen open positions.

That's how the tech job market is these days: While numerous IT vendors are laying people off, and corporate IT jobs are also being lost, other companies — both vendors and users alike — are still hiring.

But the overall trend is clear, and not encouraging: The number of IT jobs in the U.S. is shrinking. From November to December, IT employment declined by nearly 50,000 jobs, to a total of 3.85 million positions, based on an analysis of U.S. Bureau of Labor Statistics data by the National Association of Computer Consultant Businesses in Alexandria, Va. That followed a loss of almost 34,000 jobs from October to November, the NACCB said.

The contraction in the number of jobs mirrors a decline in help-wanted listings on technology job site Dice.com. Dice said it currently has about 57,000 listings, down 35% from the same time last year.

The IT labor statistics are only likely to get worse once all of the layoffs announced in January are added to the government's figures. So it's easy to miss the hiring that's going on amid the parade of workforce reductions.

Among those looking for IT help is Chris Johnson, manager of human resources at CME Group Inc., which operates the Chicago Mercantile Exchange, the Chicago Board of Trade and the New York Mercantile Exchange. Johnson has 15 IT job openings, including database and network administrator positions.

CME has received upwards of several hundred résumés for each of the available jobs, but that isn't making it easier for Johnson to find the perfect candidates to fill them.

"If somebody is good in their job, they're going to want to stay in the job that they're in," he said. "They aren't the ones papering the town with résumés right now."

So Johnson is using the LinkedIn social networking site to augment his hiring efforts. He said he's searching the site for a "passive candidate" — someone who may be advertising his IT credentials and looks like a strong match for CME, even if he isn't actively looking to leave his current job.

Even some of the large IT vendors that are making cutbacks are continuing to hire. Microsoft says its net workforce reduction will be 2,000 to 3,000 people; its careers site currently lists more than 700 open jobs in the U.S. And IBM has 3,200 jobs and internships listed worldwide, more than 550 of them in the U.S. — even as it's cutting thousands of workers in a move that it's describing as an effort to "match skills and resources with our client needs."

Other vendors are adding, not cutting, workers. For instance, Access Systems Americas Inc. in Sunnyvale, Calif., has about a dozen openings, including some for tech jobs. Access, which was previously known as PalmSource Inc., is the developer of the Garnet mobile operating system, formerly named Palm OS.

In a sign of the times, though, Access is getting significantly more applications for the open jobs than it did when the economy was in better shape. In the past, the company might have received 30 to 40 résumés for a single position, but it's getting between 60 and 70 now.

HCL America Inc., a subsidiary of India-based outsourcer HCL Technologies Ltd., is also among the vendors that are hiring. Sunnyvale-based HCL America plans to open a new service-delivery center in Cary, N.C., this month, and Shami Khorana, president of the HCL unit, said it will initially hire 100 people to work at the facility. The head count in Cary is expected to increase to 500 within five years, he added.

But not all of the jobs at the Cary facility will be new ones. Khorana said that some of the employees there will be "rebadged" workers who are shifting to HCL from customers as part of outsourcing agreements. ■

Is SharePoint enough?

In the wake of new regulations, make sure your ducks are in a row with **Autonomy ControlPoint**.

Autonomy®

Meeting Governance Needs with Autonomy ControlPoint

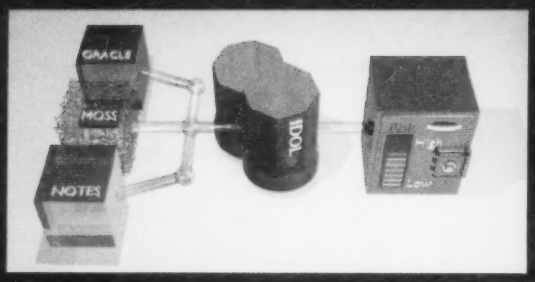
Microsoft Office SharePoint Server (MOSS) provides a portal environment for enterprises to improve departmental collaboration. It has been rapidly deployed because of its ease of installation and straightforward user interface.

Ironically, this rapid proliferation of SharePoint has led many companies to lose control of the very content they had hoped to manage. Because SharePoint is so easy to deploy, many SharePoint sites are created outside of the company's standard operating procedure for controlled information and archiving, often leading to litigation resulting from compliance violations and accidental preservation or destruction of legally relevant material.

In the wake of new regulations, sub-prime mortgage and credit crisis, and highly publicized internal fraud cases, organizations are under increased pressure to implement consistent information policies for finding, holding and disposing of content in a timely manner.

Advanced needs

Designed for easy collaboration, MOSS only addresses the "productivity" stages of the information lifecycle, with inadequate controls for maintenance and disposition of content. It lacks governance functionality including advanced needs around taxonomy creation or categorization of documents against a classification schema, which powers information management policies as well as crucial records management processes.



Applying legal hold policies within MOSS can be onerous and requires manual search and tag methods. Companies are also recognising that they have no centralized control or discovery of the information being published and collaborated on in SharePoint servers that are increasingly siloed, which can lead to severe regulatory consequences.

Autonomy, a global leader in infrastructure software for the enterprise, integrates transparently with MOSS to enhance SharePoint's information governance and eDiscovery capabilities. Autonomy ControlPoint is the industry's first information governance platform that enables real-time, policy-driven control of all SharePoint content, ensuring that customers are able to manage their SharePoint content in true alignment with today's growing corporate, legal or regulatory standards.

Critical governance tasks

ControlPoint automates critical governance tasks, including classification, preservation or disposition of information assets based on its unique ability to understand the meaning of information being shared across different SharePoint servers and other content repositories. Based on this conceptual understanding, ControlPoint automatically applies and enforces governance policies, bringing all SharePoint content under control and into compliance.

ControlPoint alleviates the need to assign teams of risk managers, legal professionals and compliance officers to manage information risk developing across SharePoint sites. It uses a centralized policy hub to enforce governance control across distributed networks, an increasingly critical function given that SharePoint servers are typically siloed throughout the enterprise.

At the heart of ControlPoint lies Autonomy's Intelligent Data Operating Layer (IDOL) Server. IDOL forms a conceptual and contextual understanding of all content in the enterprise, indexing and automatically analyzing any piece of information from over 1,000 different content formats. For the heterogeneous enterprise that holds SharePoint as just one source of data, Autonomy's mature connector framework (supporting over 400 different types of repository) enables search across the entire enterprise corpus from the SharePoint interface, allowing for an unprecedented view of the organization's information assets as well as for legally compliant searches.

With ControlPoint, all information is visible, transparent, and available to be controlled and governed. For instance, ControlPoint can perform comprehensive discovery across all information to find out what resides in SharePoint sites. It then determines what content sits outside the disposition spectrum and creates a policy to delete such information from SharePoint. ControlPoint can also discover that potentially sensitive information is not properly governed with adequate security and compliance procedures, and automatically move the content to the ControlPoint records management archive or put it on preservation should it be subject to a legal matter.

The ControlPoint policy engine can be constructed to perform automated actions, preserve and dispose of SharePoint content, and move information across SharePoint sites. ControlPoint provides full reporting functionalities, and a high-level dashboard designed for non-IT personnel that presents a holistic view of the enterprise's information governance landscape.

ControlPoint provides the flexibility to manage records in the most appropriate storage device based on the age, usage or importance of the data. This greatly reduces storage costs by eliminating the need to license costly SQL servers and alleviates the strain on network resources.

ControlPoint's integrated SharePoint client makes it easy to move content from SharePoint document libraries into the Autonomy repository while leaving a Smart Shortcut, or link behind. After migration, Autonomy manages the storage lifecycle of the SharePoint content moving it from top tier storage, through to lower cost storage, based on the rules provided by the organization's strategy.

"A Deloitte survey of more than 500 executives reveals that nearly 40 percent believe their data volume has grown to the point of being unmanageable."

—ARMA International, Information Management Newswire, September 2008

Bringing ***SharePoint*** into Compliance: Autonomy ControlPoint Highlights

With the ability to understand more than 1,000 file-types, Autonomy ControlPoint centrally manages any information asset and applies legal hold and disposition from across different SharePoint servers and other repositories on a company's wide area network. It delivers a broad set of functionalities specifically designed to address the information governance challenges with MOSS, including:

Seamless integration into SharePoint environment

Apply consistent Information Governance and eDiscovery across SharePoint and other corporate repositories with over 400 connectors and 1,000 file types supported.

Dashboard views enable automated information management

Customized dashboards provide alerting and transparency to information management processes within MOSS and throughout the enterprise, increase visibility and streamline governance actions such as legal hold and disposition.

Management of all SharePoint content in place

This eliminates the need to replicate content within SharePoint sites and from other servers. It also ensures that information related to a legal hold or regulatory matter is not accidentally deleted while in use.

Enhanced analytics, security and reporting mechanisms

Support for a rich feature-set on MOSS content such as clustering, faceted navigation and visualizations.

Improved performance

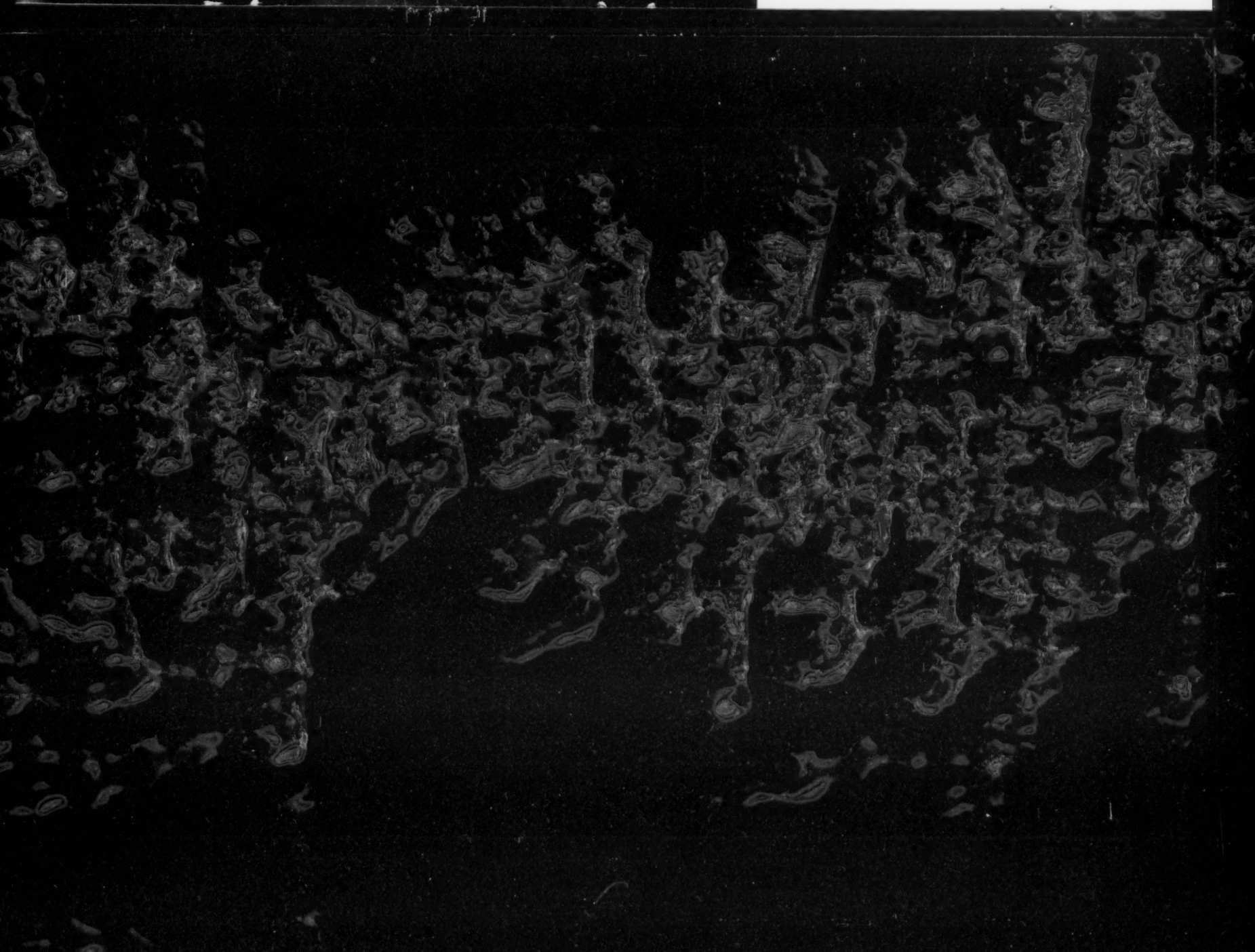
Reduce costs and improve performance over wide-area-networks by eliminating the need to store SharePoint data in SQL Server.

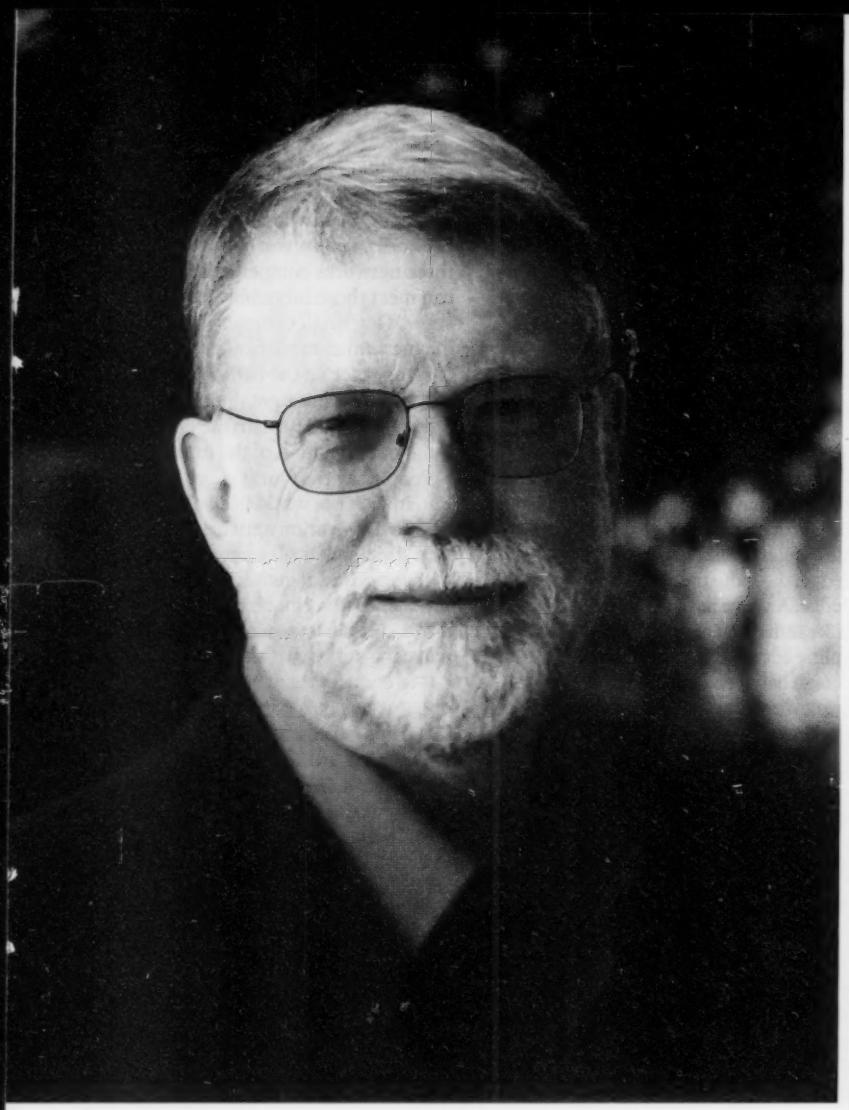
To Learn more about Autonomy ControlPoint, call 415.342.9955 or visit www.autonomy.com/controlpoint.

Named
Email and Compliance Vendor of the Year
by Financial-i

www.autonomy.com

Autonomy®





Dossier

Name: John Seely Brown

Title: Co-chairman

Organization: Deloitte Center for Edge Innovation

Location: San Jose

Favorite technology: The iPhone

In high school he was: A champion cow judger

Ambition: "Making technology disappear by designing it so that it perfectly matches your own practices and you become unaware of its existence."

Favorite nonwork pastime: BMW motorcycles

Philosophy in a nutshell: "Try to always listen with humility and listen as much to what is not being said as to what is being said."

Epitaph of choice: "That is a wow-wow" (a totally cool idea).

Latest book read: *Outliers*, by Malcom Gladwell

Best movie ever: "*The Day the Earth Stood Still* – and yes, I will see its remake."

■ THE GRILL

John Seely Brown

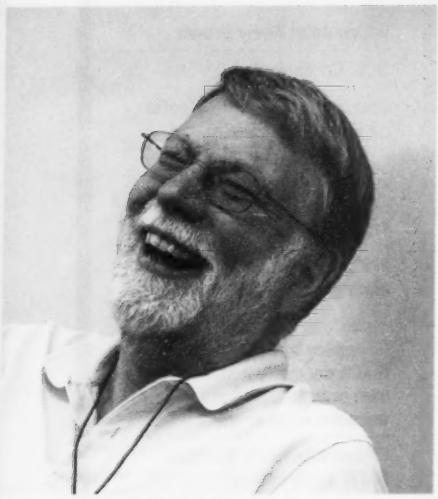
The **innovation whiz** talks about dropping **old assumptions,** finding **silver linings** and **living on the edge.**

John Seely Brown is a visiting scholar at the Annenberg School of Communication at the University of Southern California and a co-chairman of the Deloitte Center for Edge Innovation. He was previously the chief scientist at Xerox Corp. and director of the Xerox Palo Alto Research Center. His research interests include digital culture, ubiquitous computing, Web services architectures, and organizational and individual learning.

Are there any silver linings to the financial cloud we're under? Every board I'm on is terrified of the financial crisis we are in. Everybody is battening down the hatches. But I ask them, "What are the new opportunities this might provide?" Maybe it's realignments of the industry that we could help accelerate. Let's look at the opportunities on the opposite side of this.

How can you help them do that? The value lies in the questions you ask, not necessarily the problems you solve. Asking a question in a useful and productive way often gets people to discover things themselves. You get stopped by the question, and you think, "Wow, here we have stuck our heads in the sand, paying very close attention to our knitting, and we have not looked at this from the other side." There is almost always a silver lining if you ask the right question at the right time in a nonthreatening way.

What's your advice for CIOs right now? Look around and ask, "What are the



"You can get early detectors of new ideas by paying attention to the edges.

big structural changes in the IT industry? How do we use utility computing? What are the new ways to save energy? How do we start to use internal cloud computing and external cloud computing?" For example, if I'm in a start-up today, I'd not want to invest precious money in more servers. I'd be looking at how I could use the Amazon cloud in order to just pay for what I use and at the same time get a whole new kind of agility and scalability.

What is "internal" cloud computing? Shouldn't we be looking at these same ideas for dynamic reprovisioning and monitoring as a way to provide our own services? So, basically the CIO meters out pay-as-you-go, on-demand services to internal divisions. And if you do the internal utility computing right, you ought to be able to seamlessly bring in external resources on demand.

What do you mean by "edge" innovation? Edges are where the action is. There's the generational edge, where kids come up with all kinds of new ideas. They have very different work practices. How can your company leverage those practices rather than just assume they should accept your work practices? Then, at the industry level, you have edge players, often the start-ups. What are they doing that you haven't thought of? Which ones are growing shockingly fast? So, there are generational edges, the company edge, the industry edge, the market edge. And we have geographic edges, like India, and also intellectual or discipline edges. Many breakthroughs today come between disciplines, where multiple disciplines work together.

These edges are all sources of uncertainty. They are risky because they don't have road maps, and yet that's where most of the action is. You can get early detectors of new ideas by paying attention to the edges.

You say companies often react to technological change rather than proactively shape strategies. How can a big, traditional company like General Motors do that? Take health care, where there is a huge need for innovation. Suppose GM said that immediately, every doctor's office, clinic and hospital had to reveal its success measures, and then [GM] told [its] employees [it] would only reimburse them for going to those [providers] with the highest success rates. And they could say, "We'll only use those with electronic medical records, and we want the records shared among all the players in our network."

What are "innovation networks"? In Asia, these networks are constantly constructing new ideas by having hundreds or thousands of small companies in loosely coupled but long-term relationships. Many products, like the iPod and iPhone, come from original design manufacturers [ODM] in Taiwan. What most people don't realize is that when a company like HP wants a new printer or PC, they design the specs, specify the cost they want to pay and then waltz into an ODM and say, "Can you build this at this price?" The ODM knows that this same guy has been to other ODMs who have their own networks, and so you have two or three networks competing to see who can meet those incredibly aggressive specs. One small company bids on the magnesium casing, another on the RF chip, another on the battery and so on. Apple's iPhone got done that way. Steve [Jobs] had the surface design in mind but no notion of the internals.

People say the world is getting flat. But, in fact, the world is also getting spikier. Innovation networks represent tiny, local spikes of capability, which then get wired together to build a product. If you can be the first to find these rapidly developing spikes, then you can use the fact that the world is flat to connect them all together.

Could this Asian model be employed here? Everyone is talking about how to solve the General Motors problem. No one is talking about how they should work with their suppliers. The suppliers are in a vast network and are capable of tremendous innovation, but that's not how GM uses them. But look at Toyota in the U.S. Toyota keeps outperforming us not because they have better workers, but because they have figured out how to take a vast supply network from being just suppliers to being critical partners in innovation. It becomes a distributed-innovation game.

What lessons did you learn from working at Xerox PARC? First, wisdom is often the biggest obstacle to innovation. In a rapidly changing world, the assumptions that underlie our past learning may now be invalid. So, an idea that didn't work five years ago may work fantastically now.

Second, we tend to hold on to assumptions longer than we should. Often, by letting go of old assumptions, whole new vistas are created.

Third, when I was running PARC, I thought we geeks were the geniuses and people who did the marketing were not so smart. But when you have to make real innovation pay off, you often find that the genius is not in the idea creation but in the realization of that idea in the marketplace.

— *Interview by* **Gary Anthes**

■ OPINION

Scot Finnie

Apple's Silver Lining

EVEN A CURSORY REVIEW of Apple's history makes it clear that Steve Jobs has been instrumental to its success in both tours of duty. And whatever Jobs may be battling during his leave of absence, one can only hope he returns, hale and vigorous. His unbending vision has led the company to win after win.

But does that mean Apple is in trouble without him? No. In fact, Jobs or no Jobs, several opportunities exist for Apple. Here are five:

1. Deliver a lower-cost, netbook-style Mac. The pudgy, last-generation, $999 MacBook is the closest thing Apple has had to a $500 netbook. Although rumored for months, it's not clear whether Apple is building a netbook, but the time would be right. Snow Leopard, the next version of OS X, is a performance overhaul of the OS X core software. A streamlined Mac OS is precisely what you'd need to run a Mac netbook. If it happens this year, it was Jobs' initiative.

2. Foster and support independent software vendors. OS X has gone a long way toward attracting software makers to develop apps for the Macintosh. And the slowly increasing (though still small) market share for desktop Macs should help too. But Apple has had a checkered past when it comes to supporting ISVs. It could and should do more to help software makers succeed.

3. Be a lot more transparent with customers and the press. Jobs' amazing "whisper" campaigns controlled the reveal. He's a master showman who understands how to work the media and whip his audience into a frenzy. When Apple was a small company with a lot to prove, those talents were a huge asset. But Apple no longer needs to tantalize and surprise. It needs to solidify its customer base. Not everything needs to be a secret. In fact, a little more transparency would win Apple more friends.

■ Is Apple in trouble without Jobs? Not really.

4. Sell Macs to enterprise customers. This is the most challenging opportunity, with the largest potential. Apple has never sold many computers to enterprise customers. (It's tough to do that when you're not even trying.) For years, Apple lacked cost-competitive products for typical business users. But the new MacBook and the MacBook Air meet those requirements.

So, it's a funny thing. Apple finally has price-competitive products and interest from enterprise customers, but its hush-hush enterprise division — I call them the "Men in Black" — would make Howard Hughes proud. Something (or someone?) is holding it back.

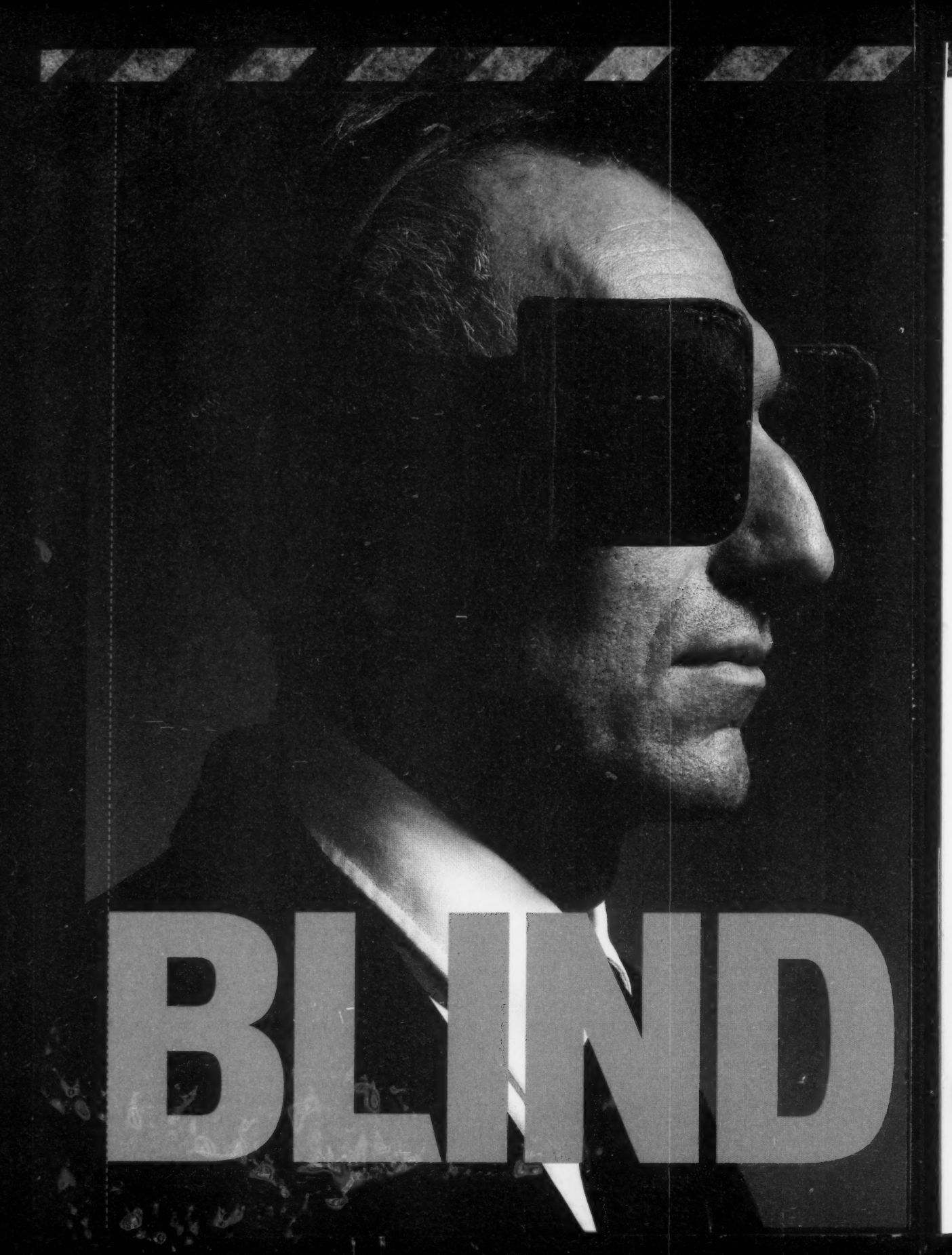
To court IT, Apple would need to reveal product road maps and stop being so secretive — but that's what nondisclosure agreements are for. It would have to add layers, such as engineering sales support, and provide business-class repair turnarounds. And it *has* made strides in those directions.

Apple doesn't have to change its identity to deal with large business customers. It doesn't have to use HP's or Dell's model. Apple could do this in its own way, and at least a modest percentage of IT customers would like it. A modest percentage is about all Apple can handle to start with anyway.

5. Get out of that exclusive AT&T deal! There are some AT&T lawyers who might object to this one. Exclusive deals are all the rage in wireless, but Verizon's network is distinctly better. Don't believe me? Check with that famous consumer magazine that prefers not to be named. Based on a survey of over 50,000 readers, it reported that Verizon had the best service in all but two major U.S. metropolitan areas. Maybe while Jobs is away, Apple can figure out a way to stop punishing its iPhone customers and cut a deal with Verizon.

But don't worry. I'm not holding my breath. ■

Scot Finnie *is Computerworld's editor in chief. Contact him at scot_finnie@computerworld.com.*


BLIND

They thought they had their stored data locked tight, but they were wrong. Here are five of the biggest storage mishaps and how you can avoid a similar fate.

By Mary Brandel

DATA BREACHES, unfortunately, have become a way of life for corporate America. According to the Identity Theft Resource Center (ITRC), 2008 saw a 47% increase in documented data breaches from the year before (see chart, page 24). And those are just the ones that made the news, says Craig Muller, an identity theft expert and founder of Identity Doctor in Irvine, Calif. "I get e-mails constantly telling me of breaches," he says.

The public is definitely feeling the pain. In a 2008 study by the Ponemon Institute in Traverse City, Mich., over half (55%) of 1,795 adult respondents across the U.S. said they'd been notified of two or more data breaches in the previous 24 months, and 8% said that they'd received four or more notifications.

But companies are still not sure how to protect themselves. In a Ponemon survey released last month, only 16% of the 577 security professionals who responded said that they were confident or very confident that current security practices could prevent the loss or theft of customer or employee data.

One way to gain confidence is to examine actual breaches and learn from them. Here's a look at five common types of breaches, with advice about how to avoid similar mishaps.

1. STOLEN EQUIPMENT

In May 2006, personal data on 26.5 million veterans was compromised when a laptop and a storage disk were stolen from the home of a subcontractor working for the U.S. Department of Veterans Affairs. Both items were recovered, and arrests were made. The FBI claimed that no data had been stolen, but the incident prompted sweeping reform at the VA. However, in January 2007, another breach occurred when a laptop was stolen from an Alabama medical facility, exposing personal data on 535,000 veterans and more than 1.3 million physicians.

SIDED!

GETTY IMAGES / JAMES PORTO

BREACHES ON THE RISE
Since 2006, the number of documented data breaches* has risen by over 40% annually.
2006
315
DOCUMENTED BREACHES
2007
446
656
2006
20 million
RECORDS EXPOSED
2007
128 million
36 million
*To qualify, breaches must include personal identifying information that could lead to identity theft, especially the loss of Social Security numbers. Five categories of data loss methods were tracked, including breaches of data on the move, accidental exposure, insider theft, subcontractor breaches and hacking.

Costs: By June 2006, the VA was burning through $200,000 a day to operate a call center to answer questions about the breach. It also spent $1 million to print and mail notification letters. It was given permission to reallocate up to $25 million to pay for those costs. Class-action lawsuits were also filed, including one demanding $1,000 in damages for each person affected. After the 2007 breach, the VA set aside an additional $20 million for breach-related costs. And the department recently agreed to pay $20 million to current and former military personnel to settle a class-action lawsuit.

Blinders: Lost or stolen equipment accounts for the largest portion of breaches — about 20% in 2008, says the ITRC. According to Bart Lazar, a partner in the Chicago office of law firm Seyfarth Shaw LLP, incidents involving lost or stolen laptops make up the majority of data-breach cases he works on.

Eye-openers: Lazar recommends restricting the placement of personal identifying information on laptops. For instance, don't tie customer or employee names to other identifiers, such as Social Security or credit card numbers; alternatively, you can truncate those numbers. Also, consider creating your own unique identifiers by, for example, combining letters from an individual's last name with the last four digits of his Social Security number.

Second, require personal information on laptops to be encrypted, despite the potential cost ($50 to $100 per laptop) and performance hit that involves, says Lazar.

This needs to be accompanied by consciousness-raising, says Blair Semple, storage security evangelist at NetApp Inc. and vice chairman at the Storage Networking Industry Association's Storage Security Industry Forum. "I've seen situations where people had the capability to encrypt but didn't," he says. "Scrambling the bits is the easy part; it's the management and deployment that's hard."

Third, Lazar recommends policies requiring very strong passwords to protect data on stolen devices.

2. INSIDER THEFT

In November 2007, a senior database administrator at Certegy Check Services, a subsidiary of Fidelity National Information Services, used his privileged access to steal records belonging to more than 8.5 million customers. He then sold the data to a broker for $500,000, and the broker resold it to direct marketers. The employee was sentenced to over four years in jail and fined $3.2 million. According to company officials, no identity theft occurred, although affected consumers received marketing solicitations from the companies that bought the data.

In another high-profile case, a 10-year veteran scientist at DuPont downloaded trade secrets valued at $400 million before leaving the company in late 2005 to join a competitor in Asia. According to court records, he used his privileged access to download about 22,000 document abstracts and view about 16,700 full-text PDF files. The documents covered most of DuPont's major product lines, including some emerging technologies. The scientist did this while in discussions with the competitor and for two months after accepting the job. He was sentenced to 18 months in federal prison, fined $30,000 and ordered to pay $14,500 in restitution.

Costs: In DuPont's case, the estimated value of the trade secrets was more than $400 million, although the government pegged the company's loss at about $180,500 in out-of-pocket expenses. There was no evidence that the confidential information was transferred to the competitor, which cooperated in the case.

According to Semple, theft of customer information is nearly always more costly than theft of intellectual property. In Certegy's case, a 2008 settlement provided compensation of up to $20,000 for certain unreimbursed identity theft losses for all class-action plaintiffs whose personal or financial information was stolen.

Blinders: Nearly 16% of documented breaches in 2008 were attributed to insiders, says the ITRC; that's double the rate of the year before. One reason for this increase is that employees are being recruited by outsiders with ties to crime — a trend that accounts for half the insider crimes committed between 1996 and 2007, according to the CERT Coordination Center at Carnegie Mellon University.

Insiders commit crimes for two reasons, CERT says: financial gain (as in the Certegy case) and business advantage (as in the DuPont case). In the latter, criminal activities usually start when the employee resigns, CERT says, but the thefts typically occur after they depart, having left secret access paths to the data they want.

Insider threats are among the hard-

Continued on page 30

ITS JOB IS TO HELP MAKE YOURS MORE PRODUCTIVE.

intel Xeon inside

Powerful. Efficient.

IBM System x3350 Express

$1,849

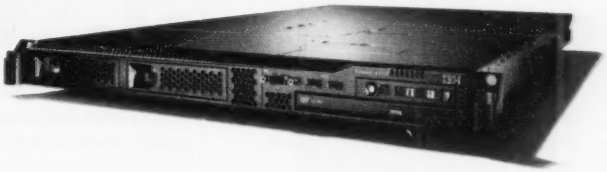
OR $48/ MONTH FOR 36 MONTHS[1]

Stop doing those routine tasks that tie you up for hours. IBM System x3350 Express monitors your infrastructure from a single point of control. Proactively identifies potential problems. And helps you solve them quickly. Let System x servers take on more routine tasks, so you can take on more challenges.

From the people and Business Partners of IBM.

It's innovation made easy.

THE SERVER THAT PRACTICALLY MANAGES ITSELF.



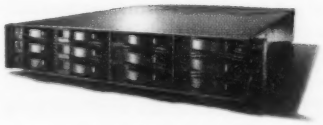
PN: 4193E2U

Featuring Intel® Xeon® Processors X3330 (2.66 GHz/1333 MHz), 6 MB L2 QC, 2x2 GB, open bay SAS 2.5" HS

Predictive Failure Analysis and Light Path Diagnostics; redundant, hot-swappable power supplies and fans; and up to 4 hard disk drives

3-year, next business day, on-site limited warranty[2]

IBM has more ways to help you get more done.



IBM SYSTEM STORAGE DS3200 EXPRESS **$4,495** OR $117/ MONTH FOR 36 MONTHS[1]

PN: 172621X

Up to six 3.5" SAS or SATA HDDs or up to eight 2.5" SAS HDDs and internal tape backup option for storage protection

Integrated RAID capability, -0, -1 and -1.0; RAID-5 optional

Comes with a 3-year on-site limited warranty[2] on parts and labor. 3-year 24x7 on-site repair (PN: 21P2078) with a 4-hour response is available for an additional $600

IBM Express "Bundle and Save"

We bundle our Express systems to give you the accessories you need – while saving you money on the hardware you want. Act now. Available through **ibm.com** and IBM Business Partners.

IBM express advantage™

ibm.com/systems/simplifyit

1 866-872-3902 (mention 6N8AH14A)

1. IBM Global Financing offerings are provided through IBM Credit LLC in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Monthly payments provided are for planning purposes only and may vary based on your credit and other factors. Lease offer provided is based on an FMV lease of 36 monthly payments. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice. 2. IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties, visit: ibm.com/servers/support/machine_warranties or write to: Warranty Information, P.O. Box 12195, RTP, NC 27709, Attn: Dept. JDJA/B203. IBM makes no representation or warranty regarding third-party products or services, including those designated as ServerProven® or ClusterProven®. Telephone support may be subject to additional charges. For on-site labor, IBM will attempt to diagnose and resolve the problem remotely before sending a technician. On-site warranty is available only for selected components. Optional same-day service response is available on [select] systems at an additional charge.

IBM, the IBM logo, IBM Express Advantage, System x and System Storage are trademarks of International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml. Intel and Xeon are registered trademarks of Intel Corporation. All other products may be trademarks or registered trademarks of their respective companies. All prices and savings estimates are based upon IBM's estimated retail selling prices as of 8.20.08. Prices and actual savings may vary according to configuration. Resellers set their own prices, so reseller prices and actual savings to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. IBM may not offer the products, features, or services discussed in this document in other countries. Prices are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or IBM Business Partner for the most current pricing in your geographic area. © 2008 IBM Corporation. All rights reserved.

Continued from page 28

est to manage, Semple says, especially when the workers use privileged access.

Eye-openers: A good precaution is to monitor database and network access for unusual activity and set thresholds representing acceptable use for different users, CERT says. That makes it easier to detect when an employee with a particular job designation does something beyond his normal duties. For instance, DuPont discovered the illegal activity because of the scientist's unusually heavy usage of its electronic data library server.

If you suspect that a breach has occurred, CERT says it's important to act quickly in order to minimize the chance of information being disseminated and to give law enforcement agencies a chance to start investigating the case.

> **"Personal information should be protected at the same level as trade secrets.**
>
> BART LAZAR, ATTORNEY, SEYFARTH SHAW LLP

Companies should also implement role-based access-control tools to maintain a high level of accountability over who is accessing valuable assets, Lazar says. Databases containing customer or employee information should allow very limited access. "How many people, on a daily basis, need to review Social Security numbers and addresses without permission?" he says. "Personal information should be protected at the same level as trade secrets."

Muller recommends using data loss prevention tools to restrict personal data from being e-mailed, printed or copied onto laptops or external storage devices. Some of these tools provide alerts that inform administrators when someone tries to copy personal data and create a log file of such an event. "In a lot of cases, companies don't have proper audit trails in place," he says.

It's also important to strengthen internal controls and audit measures by, for example, implementing iterative checks on network and database activity logs, Semple says. It's not enough to keep detailed logs; you also need audit measures in place to see if anyone has modified a log or illegally accessed it. "Unless there's some way to verify the log information wasn't tampered with, it's hard to know it's of value," he says.

But in the end, technology isn't enough. "You need to find a way to ensure users you trust are worthy of that trust," Semple says.

3. EXTERNAL INTRUSION

In January 2007, retailer The TJX Companies Inc. reported that its customer transaction systems had been hacked. The intrusions — which occurred between 2003 and December 2006 — gave hackers access to 94 million customer accounts. Stolen information was found to have been used in an $8 million gift-card scheme and in a counterfeit credit card scheme. In the summer of 2008, 11 people were indicted on charges related to the incident, which was the largest hacking and identity theft case the U.S. Department of Justice has ever prosecuted.

Costs: TJX has estimated the cost of the breach at $256 million. That includes the cost of fixing computer systems and dealing with litigation, investigations, fines and more. It also includes payments to Visa ($41 million) and MasterCard ($24 million) for losses they incurred. The Federal Trade Commission has mandated that the company undergo independent third-party security audits every other year for the next 20 years.

However, others expect that costs may rise to $1 billion, which would include the costs of legal settlements and lost customers. According to an April 2008 Ponemon study, 31% of a company's customer base and revenue source terminates its relationship with an organization following a data breach. And in its recently released annual "Cost of a Data Breach" study, Ponemon found that breaches cost companies $202 per compromised customer record last year, compared with $197 in 2007. Costs associated with lost business opportunities represented the most significant component of the increase. The average cost of a data breach in 2008 was $6.6 million, compared with $6.3 million in 2007.

Blinders: According to a 2008 Ponemon study, data breaches by hackers rank a distant fifth in terms of security threats. Indeed, about 14% of documented breaches in 2008 involved hacking, according to the ITRC. That doesn't mean companies shouldn't be wary, however.

In TJX's case, hackers infiltrated the system by "war driving" and hacking into the company's wireless network. TJX was using subpar encryption, and it had failed to install firewalls and data encryption on computers using the wireless network. This enabled the thieves to install software on the network to access older customer data stored on the system and intercept data streaming between handheld price-checking devices, cash registers and the store's computers.

Eye-openers: According to Muller, the WEP encryption that TJX used on its wireless network was insufficient — weaker even than what many home users have. "If from the parking lot you can gain access to the database, you need a higher level of data security and data encryption," he says. TJX had also stored old account information instead of permanently deleting it, Muller says.

4. NEGLIGENT EMPLOYEES

The spouse of a telecommuting Pfizer Inc. employee installed unauthorized file-sharing software on the worker's company laptop, enabling outsiders to gain access to files containing the names, Social Security numbers, addresses and bonus information of about 17,000 current and former Pfizer employees. An investigation revealed that about 15,700 people had their data accessed and copied by people on a peer-to-peer network, and another 1,250 may have had their data exposed. Because the system was being used to access the Internet from outside of Pfizer's network, no other data was compromised.

Costs: Pfizer contracted for a "support and protection" package from a credit-reporting agency, which includes a year's worth of free credit-monitoring service for those affected and a $25,000 insurance policy covering costs that individuals might incur as a result of the breach.

Blinders: Careless insiders — not malicious ones — are the No. 1 threat to data security, according to a recent Ponemon study, in which IT professionals said 88% of all breaches involved negligent insiders. "If there were more employee awareness about security, the number of breaches would come way down," Muller says. In Pfizer's case, the employee's spouse had configured the software so that other users of the file-sharing network could access files the spouse had stored on the laptop, but that gave people access to Pfizer files, too.

Combine negligent users and file-sharing software, and you've got a dangerous mix. Although most companies have outlawed P2P file sharing on their corporate networks, according to a 2007 study by Dartmouth College, many employees install it on their remote and home PCs. The study found, for example, that employees at 30 U.S. banks were sharing music and other files on peer-to-peer systems and inadvertently exposing bank account data to potential criminals on the network. Once business data is exposed, it can spread to dozens of computers around the world.

Eye-openers: First off, IT needs to either ban P2P software entirely or set policies for P2P usage and implement tools to enforce those policies. "[Pfizer] should have done a better audit of their systems to stop employees from loading any software," Muller says. "You can take away their admin rights so they can't install anything." Also important is training, he says, so users understand the dangers of P2P, what makes a good password and other standard security practices.

"There's a huge need for education so employees understand we're not trying to make things difficult but that bad things could happen," Semple notes. "It's having them understand, 'I can't do this, and here's why.' "

> **"If there were more employee awareness about security, the number of breaches would come way down.**
> CRAIG MULLER, IDENTITY THEFT EXPERT

5. SUBCONTRACTOR BREACHES

In November 2008, the Arizona Department of Economic Security had to notify families of about 40,000 children that their personal data may have been compromised following the theft of several hard drives from a commercial storage facility. The drives were password-protected but not encrypted. The agency says no information was used to commit fraud.

Costs: Subcontractor breaches are more costly than internal incidents, averaging $231 per record compared with $171, according to Ponemon.

Blinders: According to Ponemon's annual cost study, breaches by outsourcers, contractors, consultants and business partners are on the rise, accounting for 44% of all cases reported by respondents last year. That's up from 40% in 2007. In the ITRC study, 10% of breaches were associated with subcontractors in 2008.

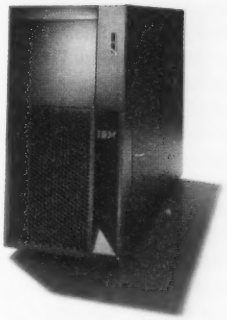
Eye-openers: Companies need to create service-level agreements that are airtight and specific, and then ensure that subcontractors are in compliance and penalize them if they aren't. In cases that involve the use of backup tapes or disks, Semple says, insist on encryption and password protection. ■

Brandel *is a* Computerworld *contributing writer. You can contact her at marybrandel@verizon.net.*

IBM express advantage

ITS JOB IS TO SIMPLIFY YOURS.

IBM System x3500 Express
$1,625



Here's another way you can become more productive. IBM System x3500 Express affordably manages your IT network from one location, identifies potential problems before they happen, and keeps your downtime to a minimum. **It's innovation made easy.**

PN: 7977E7U

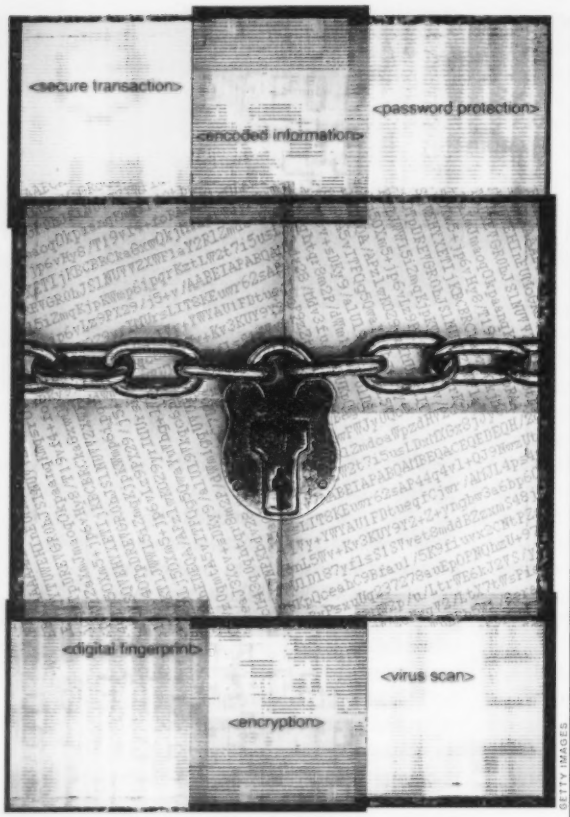
Featuring up to two Intel® Xeon® Processors E5420 2.50 GHz/1333 MHz-12 MB QC (80w) 2x1GB, keyboard and mouse, HS SAS/SATA 1 x 835W power

Up to 8 hot-swappable SAS or SATA HDDs or up to 12 hot-swappable SFF SAS or SATA HDDs to support large capacity

ibm.com/systems/simplifyit
1 866-872-3902 (mention 6N8AH15A)

IBM, the IBM logo, IBM Express Advantage, System x and System Storage are trademarks of International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml. Intel and Xeon are registered trademarks of Intel Corporation. All other products may be trademarks or registered trademarks of their respective companies. All prices and savings estimates are based upon IBM's estimated retail selling prices as of 8/20/08. Prices and actual savings may vary according to configuration. Resellers set their own prices, so reseller prices and actual savings to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. IBM may not offer the products, features, or services discussed in this document in other countries. Prices are subject to change without notice. Starting price may not include a hard drive, operating system, or other features. Contact your IBM representative or IBM Business Partner for the most current pricing in your geographic area. © 2008 IBM Corporation. All rights reserved.

intel Xeon inside
Powerful. Efficient.



GETTY IMAGES

LOCKED DOWN IN THE Data Center

Keep stored data safe within company walls with encryption and key management.

By Stacy Collett

BECU, Washington state's largest credit union, used to keep its stored data locked down using an appliance to encrypt data before it was stored to tape. But when it had the opportunity to upgrade storage equipment, the company chose a simpler, cheaper and perhaps more secure option — an application that encrypts tapes in the tape library.

The appliance "was the best solution at the time," says Kathryn Antonetti, IT systems and security manager at Tukwila-based BECU, a not-for-profit financial cooperative with assets of more than $8.5 billion. "Now encryption is being offered at virtually every layer." The switch eliminated maintenance and training costs for the appliance, and other headaches. "I had [three vendors] pointing fingers at each other" when the system had problems, she adds.

Protecting stored information is the next wave in data security. "We're starting to see more emphasis on data at rest," says Robert Rosen, former president of IBM user group Share and CIO at the National Institute of Arthritis and Musculoskeletal and Skin Diseases in Bethesda, Md. "It's kind of a no-brainer. If you've done it, your [data is] protected and you don't have to worry about it."

As companies upgrade their storage equipment, many are taking advantage of technological advances such as tape drive encryption, tape library encryption and enhancements in the way encryption keys are managed. There has also been progress in adopting the disk and tape encryption specifications of the IEEE P1619 standard, says James Damoulakis, chief technology officer at storage services provider GlassHouse Technologies Inc. "Still, it's fair to say that [storage security] has lost some momentum" because of policy and process limitations, says Damoulakis, who is a *Computerworld* columnist.

"There's a feeling that [data in storage] is a locked door — so it's not a high priority," Rosen says. "But I think that's ultimately going to change with the turnover of equipment."

"Unfortunately, most companies wait until the problem exists before fixing it," says Ari Kaplan, a senior consultant at Datalink Corp. in Chanhassen, Minn., and former president of the Independent Oracle Users Group.

With data security breaches now costing companies $202 per compromised record, according to the Ponemon Institute, it's time to start locking down data at rest. Here are three techniques for protecting stored data.

ENCRYPTION

Gartner Inc. has found that companies that encrypt stored data do so because they have to, not because they want to. "There are regulatory compliance pressures — PCI or HIPAA," says Gartner analyst Eric Ouellet, referring to the Payment Card Industry Data Security Standard and the Health Insurance Portability and Accountability Act. "Or it's the fear that the tape will fall off the back of the truck and you'll have a disclosure issue."

What's more, most encryption systems can get pricey. "When you're looking at the cost associated with this, whether it's the time to deploy or the amount of [labor] or the actual cost in dollars of the solution — these things are not cheap," Ouellet adds.

A less expensive way to add encryption is to use the capabilities that come built into many applications, Ouellet advises. "You'll have to pay for it, but it's needed, and as far as integration is concerned, it's not going to take an inordinate amount of time," he says.

Kathryn Antonetti, IT systems and security manager at credit union BECU, chose an application that encrypts tapes in the tape library.

Looking for an ultracheap approach? Ouellet suggests buying a hard drive with built-in encryption. Seagate, Toshiba and Hitachi are among the vendors introducing self-encrypting drives. "It costs only a few bucks more to buy a drive with encryption," Ouellet says. "The applications aren't even aware there's any encryption. It's all in the background at the low-level driver level."

But keep in mind that self-encrypting drives address only storage issues, Ouellet warns. "As far as the application is concerned, once it reads the data off the drive, it's in clear text — and in a backup, it's in clear text," he says. "Only in the storage environment is it safe."

On the bright side, self-encrypting drives will be helpful down the road when you have to dispose of a drive, Ouellet adds. "I can just lose or dispose of the key that was on that drive. Then the data is gone."

> **"There's a feeling that [data in storage] is a locked door – so it's not a high priority. But I think that's ultimately going to change with the turnover of equipment.**
>
> **ROBERT ROSEN,** FORMER PRESIDENT, SHARE

ON THE DESKTOP

Data at rest now includes data on the desktop. The NIH's IT department is moving to desktop-level encryption. "Unfortunately, thefts occur inside, too," Rosen says. "Encryption is a fairly simple mechanism. The performance impact is minimal."

Children's Hospital Boston also encrypts data on the desktop says Paul Scheib, director of operations and chief information security officer. "We do laptop encryption, and we try to limit what data can be stored on local machines," he says. "We don't have a sure way to stop people from writing from a CD drive, because they do have a business need to do it. The best you can do is put policies in place and educate people."

But desktop encryption resolves only one security issue, Ouellet says. "A lot of organizations have an onion-layer approach. To be able to get onto the storage environment, you have to go through a bunch of gates and barriers," such as ID management and network firewalls, he says. "That may, in fact, be good enough — it solves the external data problem. But your storage environment is not addressed that way."

KEY MANAGEMENT

For years, encryption users have been calling on security and storage vendors to offer better interoperability when it comes to managing the keys that actually control the encryption. In response, companies such as Microsoft Corp. now allow users to store the encryption keys for data held on other vendors' key management systems.

But key management will become more complex, experts say, as encryption finds its way into more and more storage devices, creating an avalanche of keys to manage.

Some industry standards are being developed, such as IEEE P1619, but they address tape encryption and not the storage environment. "We're seeing that move over to the self-encrypting drive [systems], but as far as the databases are concerned, they don't quite have a standard," says Ouellet.

For now, companies such as IBM and RSA Security Inc. provide some form of key management for external services, Ouellet says.

Industry watchers say that although companies aren't clamoring for encryption and storage security, adoption will remain steady. "There's a finite amount of resources available," Rosen says. "There won't be a huge rush to it — but with [new hardware], everything is going to be encrypted." ■

Collett *is a* Computerworld *contributing writer. Contact her at stcollett@aol.com.*

Multimaster Keys

The potential for security leaks inside a company is often overlooked, industry watchers warn. "A lot of time is focused on outside intruders, but where I see the gap is companies aren't really protecting themselves against inside threats," says Ari Kaplan, a senior consultant at Datalink and former president of the Independent Oracle Users Group. "It would be easy for disgruntled employees to get secure information from inside their company." In these cases, encryption may not be enough if the culprit is the employee holding the encryption key.

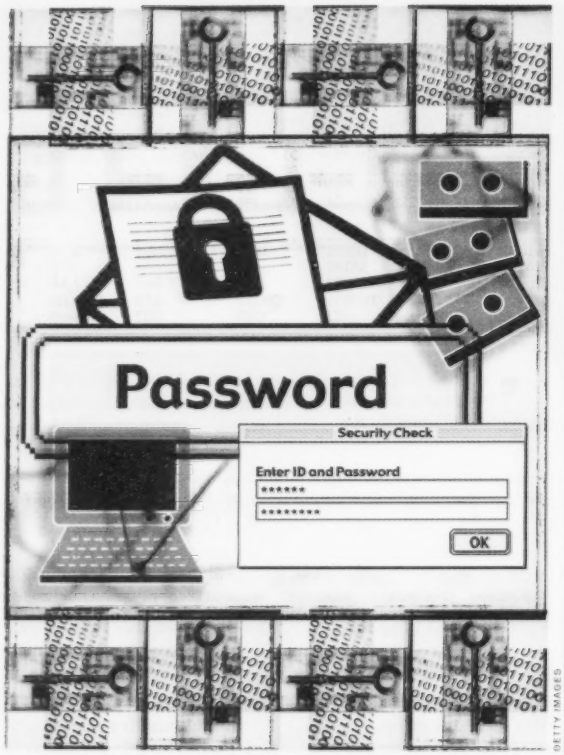
Multimaster encryption keys offer one way to plug the gap. With multimaster keys, "even if you're the DBA and know all the passwords, you still cannot retrieve the data. Only the person who manages these multimaster keys, like the CFO," has that authority, says Kaplan.

Several companies offer multimaster key solutions. Oracle's Datavault, for instance, places data into a virtual lock box. Once it goes through that area of the database, not even an admin can access it. And for compliance purposes, it ensures that data doesn't change.

Other technologies from vendors such as NetApp and Oracle keep audit trails from being altered.

Audit trails trace what information database administrators select and update as they set up a database. Of course, DBAs who are up to no good know how to cover their tracks. The newer technologies are designed to thwart such activity by preventing anyone from modifying audit trails.

– STACY COLLETT



LOCKED DOWN IN Transit

Better protect your company's movable media by rejecting these six common myths.

By Gary Anthes

EVERY FEW MONTHS, there's another horror story about lost tapes or stolen laptops, and we're left wondering if the information stored on the missing media will be put to some nefarious use, thereby adding personal injury to a public relations insult.

The importance of protecting these media has become a no-brainer. But managers are often hampered in their efforts because they buy into one or more of the following six myths of movable media:

MYTH 1: TAPES ARE OBSOLETE.

The humble magnetic tape, a seeming relic of the mainframe and batch-processing era, has given way in some instances to disk-to-disk backups to remote sites over networks. But for rapid and efficient backup, archiving and restoration of large quantities of data, there's no beating tape.

Iron Mountain Inc. offers both data backup over a network connection and tape storage at its sites. "In a disaster scenario, when time is of the essence, there is nothing more efficient than putting a collection of tapes in a vehicle and driving it to a recovery site," says Ken Rubin, a senior vice president at the information protection and storage company. "And the bandwidth limitations on transporting terabytes or petabytes of data over the line make that impractical."

Still, some users want to move on. "We are trying to get out of the tape business because of the threat of physical loss," says Christopher Leach, chief information security officer at Affiliated Computer Services Inc. He says ACS is setting up a service to send encrypted data backups to clients via a Web browser if the files aren't too big.

MYTH 2: PROTECTING TAPES AND LAPTOPS IS A JOB FOR TECHNICAL PEOPLE.

The protection of information technology is, of course, a job for IT. But there is a big and often overlooked role for others in the organization as well.

New York state CIO Melodie Mayberry-Stewart draws on a 12-person legal team to research best security practices, especially in the financial industry. Some of those people specialize in areas such as encryption and telecommunications, she says. In addition, she has a separate team of technologists who specialize in security and risk management. Mayberry-Stewart says the lawyers negotiate "painstakingly detailed" contracts and "memoranda of understanding on service levels" with companies such as Iron Mountain that transport and store the state's tapes — some 4,000 per month — from four mainframe data centers.

At Sun Microsystems Inc., tapes are created at seven data centers around the world. While each center manages its own data-retention processes, "they don't get to make up all their own rules," says Leslie Lambert, Sun's chief information security officer. So where do the rules, policies and procedures come from? "We have a very vigilant legal team, a privacy team, a business conduct team, internal auditors, external auditors and an information protection law group — all working together," she says.

Leach says keeping up with state and federal regulations on data protection and retention demands human expertise, but it's such a daunting task that he gets automated help via risk and compliance management software from Relational Security Corp.

MYTH 3: LOSING A TAPE IS PRIMARILY A SECURITY PROBLEM.

It can be a security disaster, to be sure, and it will certainly be a PR nightmare if the public finds out. But there are other equally harmful, if less dramatic, possibilities.

"If you try to decrypt your hard drive, we know it and we notify your manager.
CHRISTOPHER LEACH, CISO, AFFILIATED COMPUTER SERVICES

"I don't think so much about losing employee information [such as Social Security numbers], although that is certainly important," says Brian Lurie, IT vice president at medical products maker Stryker Corp. "What keeps me up nights is the possibility of losing a tape and then having to produce data for the FDA for a lawsuit. I worry about liability to the company from losing information that we, by law, must retain."

While the law requires that some information be kept for seven years, Stryker must retain data on customers who have Stryker products in their bodies for as long as they live, Lurie says. Although the company mirrors its disks at a remote disaster recovery center, after a certain amount of time, some data will exist only on tape transported and stored remotely by Iron Mountain.

Lurie periodically sends auditors to Iron Mountain's facility to inventory Stryker's tapes. He says regular audits are part of a three-part tape-protection program that also includes carefully crafted contracts and working with a reputable tape-storage vendor.

Experts say thefts of tapes followed by illegal usage are so rare as to be almost a nonissue. Loss of tapes through simple human error, causing processing disruptions down the line, is by far the most common problem.

MYTH 4: THERE ARE NO TECHNOLOGY SOLUTIONS; IT'S ALL ABOUT TIGHT CONTROLS.

Procedures and controls that are well thought out, automated where possible and tested are the best way to limit losses from wayward tapes and laptops, experts say. But technology can be a big help.

The primary tool remains data encryption. While the technology doesn't address Lurie's concerns about lawsuits over unrecoverable data, it's nice to be able to tell lawyers, reporters and the police that the bad guys can't do much with that laptop because the hard disk is encrypted, or with those tapes because they are unreadable.

All employee desktops and laptops at ACS are required to be "whole-disk encrypted," Leach says. "Once the disk is encrypted, we monitor it and track it, and if you try to decrypt your hard drive, we know it and we notify your manager."

ACS has more than 1 million tapes at its tape library in Dallas, and its standard practice is to encrypt their content. But, Leach says, some clients don't want to incur the cost and effort of decrypting the backup tapes they receive from ACS, so they request that the content be kept in the clear. "For those tapes, we have very strict packaging, signing and tracking at every step, almost like a chain of custody in a legal case," he says. "Tapes go into turtle boxes that are locked and unlocked at each end."

In addition, he says, "we insure them for a high amount, not because the tapes or CDs are worth a lot of money, but because that triggers tighter processes and closer scrutiny by the shipper."

Users report that they are studying new technologies to supplement or substitute for encryption. The state of New York is looking at thumbprint scans to protect laptops and tape cases. And ACS is examining prototypes of three magnetic devices that will erase the contents of tapes inside a locked case if it is broken open.

Iron Mountain says the best automated help of all may come from a tape inventory-control system to help eliminate the No. 1 cause of lost tapes — human error inside the company.

MYTH 5: ENCRYPTION IS A SILVER BULLET.

While encryption is often considered the best technical solution, it has drawbacks. For example, if you retrieve a tape but have lost the keys to decrypt it, you might be out of luck. Also, encrypting data before writing it to tape, a laptop hard drive or removable media can take copious computer resources. Finally, at many companies, encryption is optional or a requirement that can be circumvented.

For these reasons, Stryker doesn't encrypt laptop hard drives unless there's sensitive data on them. Sensitive information that remote users may need stays on protected servers, where it is accessed only when needed and not retained locally. Lurie acknowledges that this isn't perfect because it requires voluntary user compliance.

Lurie says his chores will be eased when Stryker moves to Windows Vista, because the operating system offers options for automatically encrypting data. "But it's a burden — you need additional memory, and it slows down the machine," he adds.

MYTH 6: IF YOU PROTECT YOUR TAPES AND LAPTOPS, YOU CAN FEEL SECURE.

News stories have focused attention on lost tapes and laptops, but there are a number of other devices walking out your company's door every night. Lurie says mobile devices such as BlackBerries are protected at Stryker. "I have the ability to remotely wipe them out," he explains. "If lost, we send a signal to it immediately to clear the memory."

But flash drives, CDs and DVDs are more problematic, he says. Lurie's solution: "If it's not encrypted, we just discourage the downloading of sensitive information to them."

Lurie says he even worries about the humble cell phone. "We don't allow cameras in our building, but there are lots of people who have them on their phones," he says. "If someone takes a photo of someone or something and posts it on the Internet, we've got a potential liability. I'm not sure how to deal with that yet, but I've been giving it a lot of thought." ■

Solid State's New Kill Switch

Military-grade SSDs are easier to erase, although harder to restore.

By Robert L. Mitchell

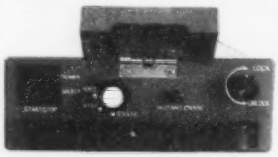
AS THE PILOT ejects inside enemy territory, the fighter jet triggers an automatic data-destruction sequence. Within 15 seconds, the highly classified mission data on the solid-state disk has been wiped out.

The storage device in this scenario didn't just burn up like the voice recorder in *Mission: Impossible*. Instead, the system's manufacturers simply took advantage of a key property of the flash memory chips that make up solid-state disks: Data can be erased much more quickly and thoroughly than it can with a magnetic, spinning hard disk. Solid-state disks, or SSDs, don't require six or seven passes to erase all traces of the bits on every track and sector. Once the bits have been reset in every flash memory cell, that data is gone forever, although meeting the most stringent government disk-sanitization requirements may still involve two or more passes.

The process is quick and efficient. "You're talking about seconds," says Gary Drossel, vice president of marketing at SiliconSystems Inc., a manufacturer of SSDs used in government systems. With a typical hard disk, just the process of getting every block on a drive of that size to spin under the read/write head would take almost an hour and a half, and the entire process could take three to four hours on a fast eSATA drive, according to experts at Texas Memory Systems Inc. and Kroll Ontrack Inc.

INSTANT ERASURE

While "fast erase" features are available today for military use, SSD manufacturers hope that the technologies will catch on for business applications such as back-end SSD storage and executive laptops. For example, computers containing sensitive data need to be scrubbed before they can be disposed of or taken out of service for maintenance. "With SSD, you can do that very quickly with little power," says Patrick Wilkison, vice president of marketing and business development at STEC Inc.



BitMicro Networks' removable SSD with backup power and a push-button erase feature.

While SSDs can typically be erased more quickly than magnetic media can be, the devices designed to meet government standards have been optimized to further speed up erasure. "We've created internal circuitry so that the host can send one command — either in software or a push button — and the drive will erase multiple chips in parallel," says Drossel. For example, it takes about 15 seconds to clear all of the chips on a 16GB SSD, he says.

Vendors have also created other schemes to meet government security requirements. BitMicro Networks Inc. offers a removable SSD with backup power that allows it to be erased up to six hours after removal from the host system.

In contrast, SiliconSystems' fast-erase feature requires power, but disconnecting the drive won't kill the process: Erasure continues the instant that power is restored. "There's no way to stop it," says Jim Handy, an analyst at semiconductor market research firm Objective Analysis. The technology can be applied to the whole drive or a preconfigured secure "zone" on the SSD that's also protected by a password.

SiliconSystems also offers an SSD self-destruct feature that applies an "overvoltage" to each of the flash chips, physically destroying them. The destruction can be triggered via software or a physical switch, says Drossel. SSDs can also be designed to self-destruct or erase if they are stolen and inserted into any unauthorized machine.

In the private sector, rapid-erasure techniques could be used in point-of-sale systems or kiosks that might contain sensitive customer or sales data. "The data may be gone, but at least it's not in the wrong hands," Drossel says.

> **"[With a fast-erase feature,] the data may be gone, but at least it's not in the wrong hands.**
>
> **GARY DROSSEL,** VICE PRESIDENT OF MARKETING, SILICONSYSTEMS INC.

MORE COSTLY RECOVERY

The flip side of the level of security SSDs offer is the fact that recovering data from them can be more difficult and expensive than for other media.

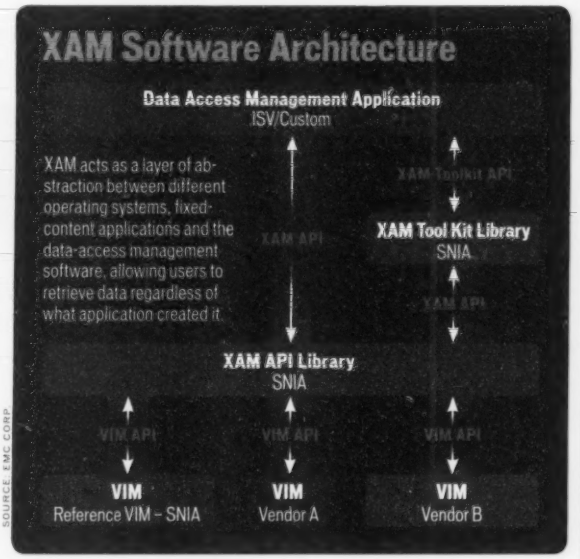
Each SSD vendor has its own proprietary method for mapping data from the file system to individual memory cells. "If you don't have the mapping table that records where everything is kept, you have random data distributed throughout the chips," says Jamon Bowen, enterprise architect at enterprise SSD maker Texas Memory Systems. "Everyone follows their own data-placement schemes. Without knowing the details of that, it would be next to impossible to piece all of that together."

That may be true for a hacker, but not for data recovery specialists, who can pull data even when an SSD has sustained physical damage. "Kroll Ontrack has developed methods to recover data without the controller chip available," says Sean Barry, senior data recovery engineer at the company. "We've been successful in discovering a number of data layouts for different manufacturers."

Another drawback is that data on SSDs can be far more costly to recover in the event of a physical failure, such as a broken circuit. "When an SSD becomes damaged, it's more difficult to get the data off the raw chips. We've had jobs go as long as three or four months," Barry says. Costs go up if the data is needed quickly and additional staffers are assigned to the project. "That jumps up the service level," he says, "and they pay accordingly." ■

Extensible Access Method

Use it to preserve the integrity and authenticity of 'fixed content.' By Russell Kay



MOST DATA is "fixed content," or digital information that will be preserved in its original form without change. Examples include most images (think of a medical X-ray or a canceled check); archived transactions; stored e-mail, presentations and business documents; and contracts, medical records and legal papers. EMC Corp. estimates that 80% of all stored data is fixed and that it grows by 90% annually.

For many organizations, federal regulations control what, how much and how long content must be retained. But for regulatory compliance, electronic discovery and corporate governance purposes, companies must be able to guarantee the integrity or authenticity of certain data, ensuring that the data we view now is the same as it was originally and hasn't changed over time.

Today's data glut, coupled with legal requirements and functional needs to store information for long periods of time, creates problems. How do we handle information from a variety of sources in different formats? What happens when technology and hardware change, making older stored data harder and more time-consuming to retrieve? When a company merges into an organization with different IT equipment and procedures, what happens to its data? And if retrieving data involves several conversion steps, how do we know it's unchanged?

A new set of standards, the Extensible Access Method, aims to bring order to this chaos. XAM acts as a layer of abstraction between different operating systems, fixed-content applications (such as e-mail, file or database archiving products), and the data-access management software. This allows users to retrieve data regardless of what application created it. XAM also simplifies the migration of data from one disk subsystem to another, obviating the need for specialized middleware.

HOW IT WORKS

XAM defines three primary objects. XSet is the basic addressable unit of data. A unique identifier is attached to data along with user-defined metadata — things like the file's creation date or size or what project the data is associated with. XAM stores metadata in separate fields and binds these to the original data, creating one data object. The user or system can specify which fields can be modified; that's critical because unmodifiable fields protect the audit trail and guarantee authenticity.

An XSystem is a logical container of XSets that can provide capabilities outside XAM's scope — such as security, migration, virtualization and performance.

The XAM Library implements an API that dynamically links applications to storage hardware. An application can communicate with multiple XAM storage systems through so-called vendor implementation modules (VIM), which are similar to device drivers. These pieces of vendor-written code translate XAM requests into device-specific actions. Thus, vendors needn't change products to use XAM; instead they can write VIMs and let XAM handle everything else.

XAM uses a query language, XAM QL, modeled on the SQL's Select statement. XAM queries aren't as powerful as SQL's general-purpose queries because XAM storage systems are generally designed as data archives, not as relational databases.

XAM grew out of an EMC system called Centera, which began shipping in 2002 and focused on fixed-content data. IBM grew interested in 2004, and Hewlett-Packard, Hitachi and Sun Microsystems joined the effort in 2005, at which time XAM was proposed to the Storage Networking Industry Association (SNIA) as a formal interface. As XAM developed, it grew to encompass non-fixed-data content.

In October 2007, SNIA announced successful interoperability demonstrations with hardware and software from EMC, HP, Sun and Vignette. According to SNIA, this showed that XAM can decouple data applications from storage systems, freeing user organizations from being locked into a single supplier on either end. ■

Kay *is a* Computerworld *contributing writer. Contact him at russkay@charter.net.*

Definition

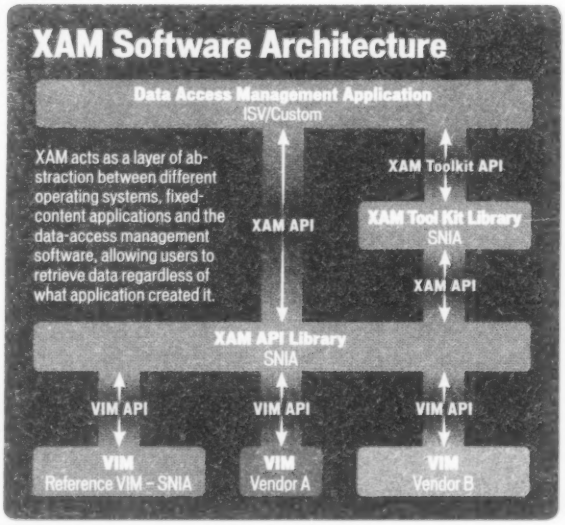
XAM (Extensible Access Method) is a set of standards and a programming interface for storing fixed-content information so that it can be retrieved by many applications and management software, and so its integrity can be guaranteed and verified.

COMPUTERWORLD.COM

WANT MORE?
For a complete archive of QuickStudies, go to **computerworld.com/quickstudies**

Extensible Access Method

preserve the integrity and authenticity



XAM (Extensible Access Method) is a set of standards and a programming interface for storing fixed-content information so that it can be retrieved by many applications and management software, and so its integrity can be guaranteed and verified.

FIXED DATA is "fixed content," or digital information that will be preserved in its original form without change. Examples include most images (think of a medical X-ray or a canceled check); archived transactions; stored e-mail, presentations and business documents; and contracts, medical records and legal papers. EMC Corp. estimates that 80% of all stored data is fixed and that it grows by 90% annually.

For many organizations, federal regulations control what, how much and how long content must be retained. But for regulatory compliance, electronic discovery and corporate governance purposes, companies must be able to guarantee the integrity or authenticity of certain data, ensuring that the data we view now is the same as it was originally and hasn't changed over time.

Today's data glut, coupled with legal requirements and functional needs to store information for long periods of time, creates problems. How do we handle information from a variety of sources in different formats? What happens when technology and hardware change, making older stored data harder and more time-consuming to retrieve? When a company merges into an organization with different IT equipment and procedures, what happens to its data? And if retrieving data involves several conversion steps, how do we know it's unchanged?

A new set of standards, the Extensible Access Method, aims to bring order to this chaos. XAM acts as a layer of abstraction between different operating systems, fixed-content applications (such as e-mail, file or database archiving products), and the data-access management software. This allows users to retrieve data regardless of what application created it. XAM also simplifies the migration of data from one disk subsystem to another, obviating the need for specialized middleware.

HOW IT WORKS

XAM defines three primary objects. XSet is the basic addressable unit of data. A unique identifier is attached to data along with user-defined metadata — things like the file's creation date or size or what project the data is associated with. XAM stores metadata in separate fields and binds these to the original data, creating one data object. The user or system can specify which fields can be modified; that's critical because unmodifiable fields protect the audit trail and guarantee authenticity.

An XSystem is a logical container of XSets that can provide capabilities outside XAM's scope — such as security, migration, virtualization and performance.

The XAM Library implements an API that dynamically links applications to storage hardware. An application can communicate with multiple XAM storage systems through so-called vendor implementation modules (VIM), which are similar to device drivers. These pieces of vendor-written code translate XAM requests into device-specific actions. Thus, vendors needn't change products to use XAM; instead they can write VIMs and let XAM handle everything else.

XAM uses a query language, XAM QL, modeled on the SQL's Select statement. XAM queries aren't as powerful as SQL's general-purpose queries because XAM storage systems are generally designed as data archives, not as relational databases.

XAM grew out of an EMC system called Centera, which began shipping in 2002 and focused on fixed-content data. IBM grew interested in 2004, and Hewlett-Packard, Hitachi and Sun Microsystems joined the effort in 2005, at which time XAM was proposed to the Storage Networking Industry Association (SNIA) as a formal interface. As XAM developed, it grew to encompass non-fixed-data content.

In October 2007, SNIA announced successful interoperability demonstrations with hardware and software from EMC, HP, Sun and Vignette. According to SNIA, this showed that XAM can decouple data applications from storage systems, freeing user organizations from being locked into a single supplier on either end. ■

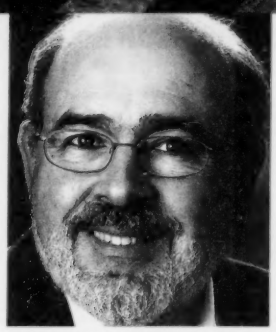
Kay is a Computerworld contributing writer. Contact him at russkay@charter.net.

COMPUTERWORLD.COM

WANT MORE? For a complete archive of QuickStudies, go to computerworld.com/quickstudies

James Damoulakis

Your Security Game Plan



HOW MUCH PROGRESS is really being made in securing storage? For several years now, pundits have sounded the alarm about a range of security risks associated with storage. That includes everything from a lack of fundamental network security practices for SANs to the ever-familiar problems associated with handling off-site media. Regarding the latter, hardly a week goes by that some organization isn't reporting the loss or theft of laptops or tapes containing confidential information.

Yet, aside from those corporate victims in the spotlight that have been forced to make improvements, it seems that the state of storage security has been advancing very slowly.

Furthermore, many so-called storage security initiatives should be more accurately labeled as off-site tape security initiatives. In other words, the focus isn't on a strategic approach to securing the overall storage infrastructure, but on the pain point du jour — in this case, the desire to avoid being the next organization to make headlines in *Computerworld* for the wrong reason. Certainly, the desire to close this particular security hole is understandable, but without an overall game plan, there is a strong likelihood that efforts will be duplicated and other risks overlooked.

A widely reported study from the Identity Theft Resource Center found a 47% increase in data breaches in 2008 compared with 2007. Of these breaches, 20.7% involved "data on the move" — on laptops or tapes, for example. However, twice as many incidents (41%) occurred through a combination of hacking, insider theft and subcontractor breaches.

Yet even the goal of securing off-site media hasn't been successfully addressed. Consider, for example, the lack of widescale adoption of encryption. Only 2.4% of the lost media in the above study was encrypted. Why is that? In the case of tape, it's not because of a lack of awareness or misunderstanding the problem — that's painfully obvious. Nor is it because of a lack of technology available to address the problem. Encryption products for every level can be obtained from mainstream vendors: tape drive (LTO-4, IBM TS1130 or STK T10000), tape library (Spectra Logic), SAN switch (Cisco or Brocade), SAN or LAN appliance (NetApp) and host software (most backup applications).

■ The problems of key management point to a larger organizational issue: the lack of a comprehensive security strategy that truly encompasses storage.

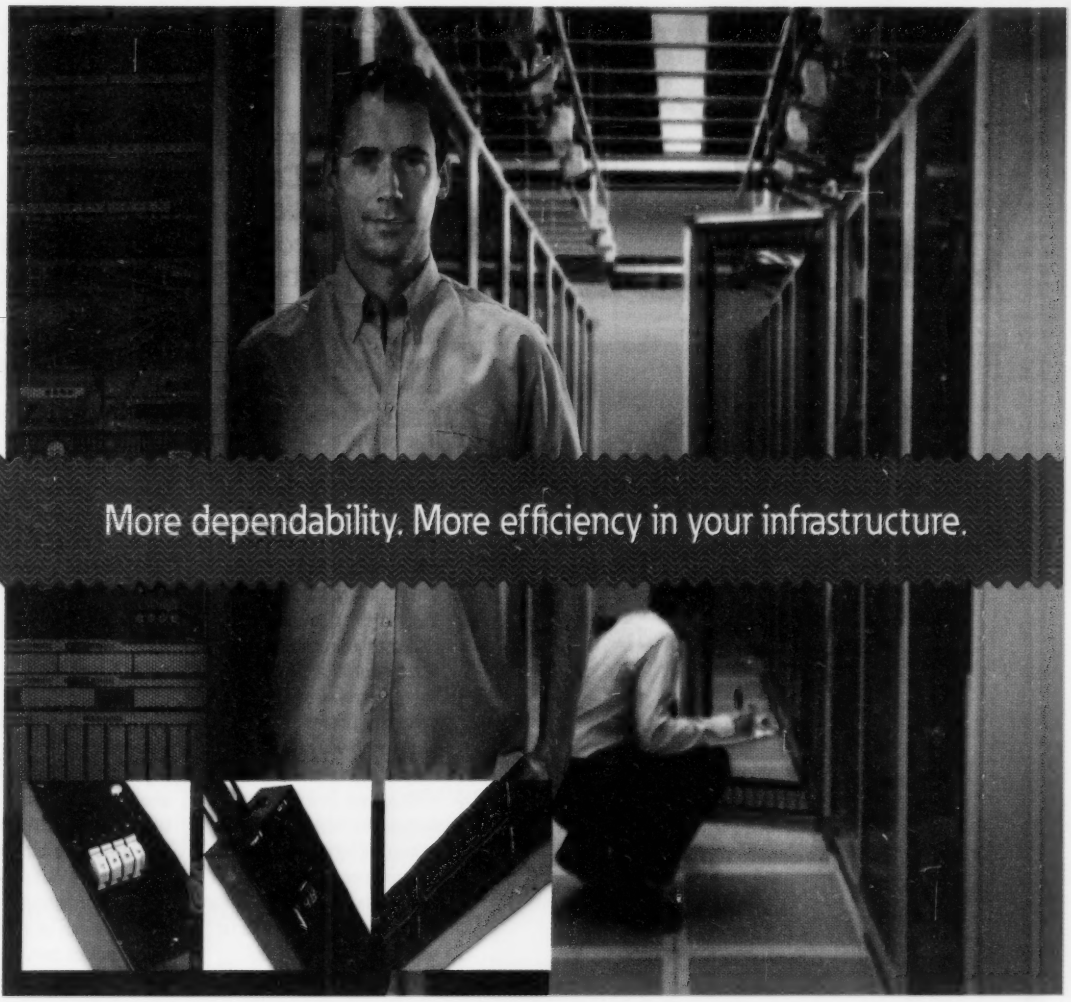
It's easy to point to the challenges of key management as the primary roadblock to more widespread adoption of media encryption, and this is certainly a contributing cause. However, the problems of key management point to a larger issue: the lack of a comprehensive security strategy that truly encompasses storage. As long as storage sits at the periphery of organizations' security focus, there will continue to be risks, and obstacles to addressing those risks.

What's required is understanding that different entities within an enterprise access, manage, control and own responsibility for data. An effective strategy considers the security needs of all constituents.

A strategic approach to storage security not only would weigh additional risks beyond things like off-site media encryption, but would also consider identifying which data needs to be encrypted and at what level. Perhaps if data is encrypted at the application level to protect against unauthorized access, it might not need to be re-encrypted at the tape level. If a centralized key-management function, with associated policies and processes, were instituted to manage all data security access, the prospect of off-site tape encryption wouldn't be as daunting.

Given the current economic reality, it's improbable that many organizations will undertake this type of program in the near future. However, it's important to begin to bridge the gap between storage and security and build a rational framework on which to incrementally improve. Otherwise, the breach tally is certain to climb even higher in 2009. ■

James Damoulakis *is chief technology officer at GlassHouse Technologies Inc., an IT infrastructure consulting and services firm.*



Eaton makes selecting Enclosure Power Distribution Units easy

Uninterruptibility from Eaton® isn't a new offering. It's an iron-clad promise, backed by a $13B global organization and a century-long heritage with power protection, distribution and management expertise.

Eaton's expanded portfolio of power distribution units (ePDU™) offers the broadest range on the market. Making the right decisions from the start can make a difference in the dependability and efficiency of your infrastructure.

Use our new product configuration wizard to search over 1,000 products for the perfect solution. Tailor your ePDU to include a wide range of voltages using various combinations of NEMA and IEC outlets and plugs.

Visit the product wizard to meet your power distribution challenges and ***power through***.

www.epdu.com/cw

(877) 785-4994

EATON
Powering Business Worldwide

Eaton and ePDU are trademarks of Eaton Corporation. ©2008 Eaton Corporation. All rights reserved.

Career Watch

Rise of the 'Nanobots'

No, they aren't those hypothetical molecular-scale robots that could someday be introduced into our bloodstreams to fix what ails us. These so-called nanobots are office workers, including some IT professionals. Or, more precisely, they are workers who are hardly ever in the office. The somewhat fanciful acronym for this category of worker is derived from Nearly Autonomous, Not in the Office, doing Business in their Own Time Staff. The coiners of the term are two New Zealand researchers, David Pauleen and Brian Harmer, who wrote about nanobots in the Dec. 14 issue of the *MIT Sloan Management Review*. They say nanobots are highly dependent on mobile devices and remote access to the corporate network, but unlike run-of-the-mill mobile workers, they aren't required to stay in close contact with managers. Instead, nanobots are entrusted with unusual levels of personal freedom while they're on the job, in return for which they're almost always on the job.

– JAMIE ECKLE

WHY WORKERS LEAVE

Executives were asked, "Which of the following is most likely to cause good employees to quit their jobs?" Here are their responses:

	2009	2004
Unhappiness with management	**35%**	**23%**
Limited opportunities for advancement	**33%**	**39%**
Lack of recognition	**13%**	**17%**
Inadequate salary and benefits	**13%**	**11%**
Bored with their jobs	**1%**	**6%**
Other/don't know	**5%**	**4%**

SOURCE: ROBERT HALF TECHNOLOGY SURVEY BASED ON INTERVIEWS WITH 150 SENIOR EXECUTIVES AT THE 1,000 LARGEST COMPANIES IN THE U.S.

PAGE COMPILED BY JAMIE ECKLE.

■ **Q&A**

Tony Lee

The **publisher** of **CareerCast.com** and **JobsRated.com** discusses the sites' recent **ranking of occupations,** which put two **IT jobs** in the top 10.

What sorts of criteria were used? To quantify the many facets of the 200 jobs included in our report, we determined and reviewed various critical aspects of all of the jobs, categorizing them into five core criteria – that is, the general categories that are inherent to every job: work environment, income, outlook, stress and physical demands. Many smaller criteria are included in these core areas, and all are weighted and reviewed by our team of researchers. One overarching theme is that the more control you have over your daily activities, the higher that job tends to rank. So if you have a boss looking over your shoulder or frequent tight deadlines that have to be met, your job will lose points in the rankings. [Note: The full methodology is explained at *www.CareerCast.com/jobs/content/JobsRated_Methodology*.]

A lot of people in the technology field would be surprised to see "software engineer" at No. 5, given that such positions are increasingly being offshored. Did it score high for job security? Job security was its lowest score, but it scored so high in the other categories, it landed at No. 5. Software engineer scored highest for work environment. The majority of software engineers work in nice offices, with a cafeteria nearby, and [they] can do things like listen to music via headphones, which is far nicer than many other jobs. It also ranked high for income, with an average of $86,139.

It sounds like the more sedentary a job, the higher it ranked. But is physical activity really a drawback in a job? Not necessarily, as long as the physical activity doesn't frequently lead to injury. For instance, petroleum engineers and geologists both often work outside the office but still rank among the top 30 best jobs, since it's unlikely their outside work will lead to harm or is done in uncomfortable weather.

The economy has shifted quickly over the past few months. Do you have a sense of how those changes might affect the rankings if you were to take a new look today? We kept following the data right through the fall, so while there may be a few small changes since then, the data should be up to date.

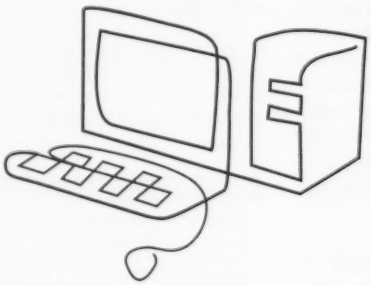
– JAMIE ECKLE

THE 10 BEST JOBS

1	**Mathematician**
2	**Actuary**
3	**Statistician**
4	**Biologist**
5	**Software engineer**
6	**Computer systems analyst**
7	**Historian**
8	**Sociologist**
9	**Industrial designer**
10	**Accountant**

SOURCE: CAREERCAST.COM RANKING OF OCCUPATIONS, SEPTEMBER 2008

Co-Branded
EMAIL
BLASTS



Reach your target audience of professional IT job seekers with Computerworld's Co-Branded Email Blasts. This unique program allows you to choose your criteria of 100% opt-in subscribers by geography, company size, job title and industry.

Call Dawn Cora at
800-762-2977 for details!

COMPUTERWORLD

Thomson Inc. is seeking a Software Engr for its El Segundo, CA ictn to be resp for taking s/w devlpnt processes through latter stages of consumer electronics lifecycle from initial integration through high vol mfg to on-going prodct maintenance & trouble-shooting. Must have a Master's deg or equiv in EE or rltd fld + 1 yr wk exp in rlt occuptn of engineering & complex s/w system designs. Salary DOE. Send cov ltr & resume to Thomson Inc., HR – Job #9051, 101 W. 103rd Street, Indianapolis, IN 46290.

COMPUTERWORLD

Law Firms
IT Consultants
Staffing
Agencies

Are you frequently placing legal or immigration advertisements?

Let us help you put together a cost effective program that will make this time-consuming task a little easier.

Contact us at:
800.762.2977
IT|careers

Computer Professionals needed (Plainsboro) NJ based IT firm, Jr. Lvl positions Programmer Analysts, S/w Engineers, Systems Analysts, and Business Analyst to develop, create, and modify general comp. Applications s/ware or specialized utility programs. Analyze user needs and develop software solutions. Sr. Lvl position, Sr. Software Engineers, Sr Programmer Analyst, Sr. Business Analyst, Sr Systems Analyst to plan, direct, or coordinate activities in such fields as electronic data processing, information systems, systems analysis, and computer programming. Apply w/2 copies of resume to MCS Global, Inc 666 Plainsboro Rd, Suite # 525, Plainsboro, NJ-08536.

Computer Professionals needed (Bristol, PA) IT firm, Jr. Lvl positions Programmer Analysts, S/w Engineers, Systems Analysts, Business Analyst, Database Administrators to develop, create, & modify general comp. applications s/ware or specialized utility programs. Analyze user needs & develop s/w solutions. Sr. Lvl position, Sr. Programmer Analyst, Sr. S/w. Eng, Sr. Business Analyst to plan, direct, or coordinate activities in such fields as electronic data processing, information systems, systems analysis, & computer programming. Apply w/2 copies of resume to HRD Synchron Systems, Inc, 1250 Veterans Hwy, Suite # G16, Bristol, PA - 19007

Project Manager. Plan/direct vendor mgmt. in sales performance, implementations web-products. Direct activities of personnel to ensure progress schedule, budget. Req. MBA w/1 yr. exp. or as a MRA concentration in IT industries w/web-products. Work area: Southfield, MI

Project Manager. Coordinate team supporting global fraud prevention initiatives utilizing artificial intelligence technologies. Review proposals. Tools: MS Project, MS Office, C, C++, JAVA, XML, SQL, MQ Access, Oracle Plus, Quality Center, UNIX, and Windows. Req. Master's Comp. resource Info. Mgmt. w/1 yr. exp. or as a Systems analyst worked on fraud prevention projects. Work area: O'Fallow, MO.

Jeem Solutions. Fax resume to 877-581-1833

Thomson Inc. is seeking a Member Technical Staff (Electrical Engineer) for their Princeton, NJ ictn to devlp new frameworks for advncd terminals & mobile applctns. Must have a Master's deg or equiv in EE or rltd fld + 1 yr of exp in the rltd occptn of Windows mobile, FLUTE/DVB-H protocols, DirectFB & QT, & ARM compiler, or a Bach deg in EE or rltd fld + 5 yrs of exp in the rltd occptn of Windows mobile, FLUTE/DVB-H protocols, DirectFB & QT, & ARM compiler. Exp may have been gained prior to completion of master's deg. Salary DOE. Send cov ltr & resume to Thomson Inc., HR – Job #9048, 101 W. 103rd Street, Indianapolis, IN 46290.

Computer Professional (Plainsboro, NJ): Jr. Level positions– Programmer Analyst, software Engineer, Systems Analyst: Design, develop, test, create & modify comp. Applications S/w. Analyze user needs & develop S/w solutions. Sr. Level Positions – Project Leader, Team Manager, MIS Manager: Plan, design, dvlp, direct enhance, customize, supervise & coordinate to implement advance S/w applications/ modules in complex computer environments.Apply in duplicate to HR,Millennium Information Technologies Inc.101 Morgan Lane, Suite # 204, Plainsboro NJ 08536 USA

Systems Librarian (Houston, Texas) Provide database system administration and support for integrated library systems and servers. Install software updates and setup and maintain user accounts. Coordinate server problems with the UNIX team. Perform regularly scheduled backups. Participate in planning for the next generation database. Maintain test system with latest SIRSI. Master's degree in Library Science or Library Information Science and experience required. Apply: Rice University http://jobs.rice.edu (Requisition # 0900A)

Computer Professionals needed (Edison, NJ) IT firm, Jr. Lvl positions Programmer Analysts, S/w Engineers, and Systems Analysts, Business Analyst, to develop, create, and modify general comp. applications s/ware or specialized utility programs. Analyze user needs and develop software solutions. Sr. Lvl position, IT Manager, MIS Manager, to plan, direct, or coordinate activities in such fields as electronic data processing, information systems, systems analysis, and computer programming. Apply w/2 copies of resume to HRD Infokall, Inc, 510 Thornall Street, Suite # 260, Edison, NJ – 08837.

IT PROFESSIONALS needed w/exp for unanticipated client sites: IT Project Mgrs, Web Services Project Mgrs, Web Engrs, QA Project Mgrs, Business Systms Analysts & J2EE Dvlprs. Mail resume, specifying position applying for to: Collabera, Attn: Hireme, 25 Airport Rd, Morristown, NJ 07960

Shark Tank

TRUE TALES OF IT LIFE AS TOLD TO SHARKY

How It Works, Really

Vendor sends this IT pilot fish a cheap digital camera as a "thank you" gift for sending business his way. And fish, who has never received any vendor gifts before, shows it to his boss to make sure everything is OK. "My boss was not happy," says fish. "He began telling me the company policy about accepting gifts from vendors and told me to send it back – which I did." Fast-forward several weeks: Fish is solving an e-mail problem on a VP's PC when he notices that she is asking a vendor to supply her with complimentary tickets for a local sports event. Fish returns to his boss and asks for clarification about the vendor-gift policy. Boss reads it to him. The penalty for failure to follow the policy: termination. Several weeks later, fish is at the sports event when he spots the VP and her husband in very good seats – right next to fish's boss. "I acted surprised and walked over to talk," fish says. "Seems the VP got the tickets for the boss, the boss's wife, herself and her husband. The boss suggested that she talk to the vendor to get the tickets."

Efficiency

This data center is being relocated, and movers are scheduled to transport four $75,000 UPS units on a 600-mile trip. "I happened to be looking out the window at the parking lot," fish says. "I spotted several men loading the UPS units onto a grass-stained landscaping equipment trailer. I took a deep breath and, trying not to imagine the prospect of our valuable assets racing down I-95 with bungee cords flapping in the breeze, went running into my boss's office." Once there, fish calls the moving company – which informs him that its truck hasn't arrived yet. As fish and his boss run outside to confront the movers, they spot another tenant approaching the trailer too. "Their company was also moving, and the landscapers were actually hired by them," says fish. "We breathed a sign of relief as we spotted our moving truck pulling into the parking lot."

Two Layers, Right?

It's 7 a.m. at this engineering firm, and a senior pilot fish is the only IT guy around when a call comes in from the boss of the production department. "She was complaining about a new dual-layer DVD burner that a tech had recently installed," says fish. First she tells fish that the new DVD-burning software is too difficult to use. Then she claims the drive itself is broken and won't burn a disk. Seeing scraps of stick-on labels on the user's desk, fish pops open the DVD tray to examine the media. Sighs fish, "For some reason, she had attached labels to both sides of the DVD."

■ *Feed the Shark! Send me your true tale of IT life at sharky@computerworld.com. You'll get a stylish Shark shirt if I use it.*

COMPUTERWORLD.COM

DO YOU LOVE SHARK TANK?
Then you might like Shark Bait, too. Dive in and dish the dirt with like-minded IT pros.
sharkbait.computerworld.com

CHECK OUT Sharky's blog, browse the Sharkives and sign up for Shark Tank home delivery at **computerworld.com/sharky.**

■ COMPANIES IN THIS ISSUE

Page number refers to page on which story begins. Company names can also be searched at computerworld.com

Access Systems Americas Inc. 18
Acumen Solutions Inc. 16
AdaptaSoft Inc. 10
Advanced Micro Devices Inc. 6
Affiliated Computer Services Inc. 34
Amazon.com Inc. 24
Annenberg School of Communication 23
Apple Inc. 24, 25
Ariba Inc. 16
Arizona Department of Economic Security 31
Association of Computer Consultant Businesses 18
AT&T Inc. 25
Automated HealthCare Solutions Inc. 18
Automatic Data Processing Inc. 16
Avendus Capital Inc. 10
BECU 32
BitMicro Networks Inc. 36
Brocade Communications Systems Inc. 38
CA Inc. 4
CareerCast.com 40
Carnegie Mellon University 28
CBI Health 10
CERT Coordination Center 28
Certegy Check Services Inc. 28
Children's Hospital Boston 33
Cisco Systems Inc. 38
CME Group Inc. 18
Dartmouth College 31
Datalink Corp. 32, 33
Dell Inc. 10, 25
Deloitte Center for Edge Innovation 23
Delta Air Lines Inc. 10
Dice Holdings Inc. 18
Directions on Microsoft 6
DuPont 28
EMC Corp. 37
FBI 27
Federal Trade Commission 30
Fidelity National Information Services 28
Ford Motor Co. 10
Forrester Research Inc. 8, 12
Gartner Inc. 6, 16, 32
General Motors Corp. 24
GlassHouse Technologies Inc. 32, 38
HCL America Inc. 18
HCL Technologies Ltd. 10, 18
Hewlett-Packard Co. 24, 25, 37
Hitachi Ltd. 33, 37
Hope Foundation 4
IBM 8, 18, 32, 37, 38
IDC 12, 16
Identity Doctor 27
Identity Theft Resource Center 27, 38
iGate Corp. 10
Independent Oracle Users Group 32, 33
Institute of Electrical and Electronics Engineers Inc. 32
Intel Corp. 8, 10
Iron Mountain Inc. 34
JobsRated.com 40
Kroll Ontrack Inc. 36
Lawrence Livermore National Laboratory 8
Lenovo Group Ltd. 10
LinkedIn Corp. 18
Mane USA Inc. 16
MasterCard International Inc. 28
Mesabi Group 10
Microsoft Corp. 6, 18, 33
Mozilla Corp. 8
National Association of Computer Consultant Businesses 18
National Institutes of Health 32
NetApp Inc. 28, 33, 38
New York Mercantile Exchange Inc. 18
Objective Analysis 36
Oracle Corp. 8, 32, 33
Pfizer Inc. 30
Ponemon Institute 6, 27, 32
Progress Software Corp. 16
Relational Security Corp. 34
Robert Half Technology 40
Roche Holding Ltd. 8
RSA Security Inc. 33
Salesforce.com Inc. 12
SAP AG 8
Satyam Computer Services Ltd. 10
Seagate Technology LLC 10, 33
Seyfarth Shaw LLP 28
Sharp 32
SiliconSystems Inc. 36
Sonoco Products Co. 16
Spectra Logic Corp. 38
Springs Valley Bank & Trust Co. 16
STEC Inc. 36
Storage Networking Industry Association 28, 37
Stryker Corp. 35
Sun Microsystems Inc. 10, 34, 37
Texas Memory Systems Inc. 36
The Boston Consulting Group Inc. 10
The Goldman Sachs Group Inc. 10
The TJX Companies Inc. 30
Toshiba Corp. 33
Toyota Motor Corp. 24
Trusted Computing Group 10
U.S. Army 16
U.S. Bureau of Labor Statistics 18
U.S. Department of Energy 8
U.S. Department of Justice 30
U.S. Department of Veterans Affairs 27
U.S. Food and Drug Administration 35
Unicorn HRO Inc. 16
Unisys Corp. 10
University of Southern California 23
Verizon Communications Inc. 25
Vignette Corp. 37
Visa Inc. 28
Xerox Corp. 23

ADVERTISER INDEX

Autonomy 19-22
www.autonomy.com/controlpoint
CommVault 14-15
www.commvault.com/simpana
Estor! Corporation 39
www.aprilu.com/cw
IBM Express Seller 29, 31
ibm.com/systems/simplify/t
IBM IT Campaign 7
ibm.com/green/software
IBM IT Campaign 9
ibm.com/green/info
IBM IT Campaign 11
ibm.com/green/services
InterSystems 13
InterSystems.com/Connect18A
Microsoft Unified Communication C2-1
microsoft.com/voip
NEC C4
www.necus.com/uc
NetApp C3
netapp.com/efficiency
SAS 3
www.sas.com/starfish
SunGard Availability Services 17
www.availability.sungard.com

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

Periodical postage paid at Framingham, Mass., and other mailing offices. Posted under Canadian International Publication agreement PM40063731. **CANADIAN POSTMASTER:** Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A 7C9. Computerworld (ISSN 0010-4841) is published weekly, except for combined issues in November and the last week and first week of each of the following months: December/January, March/April, May/June, June/July, and August/September by Computerworld, Inc., 1 Speen Street, Box 9171, Framingham, Mass. 01701-9171.

Copyright 2009 by Computerworld Inc. All rights reserved. Computerworld can be purchased on microfilm and microfiche through University Microfilms Inc., 300 N. Zeeb Road, Ann Arbor, Mich. 48106. Computerworld is indexed. Back issues, if available, may be purchased from the circulation department. Photocopy rights: permission to photocopy for internal or personal use is granted by Computerworld Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of $3 per copy of the article, plus 50 cents per page, is paid directly to Copyright Clearance Center, 27 Congress St., Salem, Mass. 01970. Reprints (minimum 100 copies) and permission to reprint may be purchased from Ray Trynovich, Computerworld Reprints, c/o The YGS Group, Greenfield Corporate Center, 1808 Colonial Village Lane, Lancaster, Pa., 17601, (800) 290-5460, Ext. 148, Fax: (717) 399-8900. Web site: www.reprintbuyer.com. E-mail: computerworld@theygsgroup.com. Requests for missing issues will be honored only if received within 90 days of issue date. Subscription rates: $8 per copy; U.S. – $99.99 per year; Canada – $130 per year; Central & So. America, $250 per year; Europe – $295 per year; all other countries – $295 per year. Subscriptions call toll-free (888) 559-7327. **POSTMASTER:** Send Form 3579 (Change of Address) to Computerworld, PO Box 3500, Northbrook, Ill. 60065-3500.

BPA WORLDWIDE ABM

COMPUTERWORLD

HEADQUARTERS
P.O. Box 9171, 1 Speen Street
Framingham, MA 01701-9171
(508) 879-0700
Fax (508) 875-4394

President/CEO
Matthew J. Sweeney
(508) 271-7100

Executive Assistant to the President/CEO
Diana Cooper
(508) 820-8522

Vice President/Publisher Integrated Programs & Events
John Amato
(508) 820-8279

Vice President/ General Manager Online
Martha Connors
(508) 620-7700

Vice President, Marketing
Matt Duffy
(508) 820-8145

Editor in Chief
Scot Finnie
(508) 628-4868

Vice President, Custom Content
Bill Laberis
(508) 820-8669

Vice President, Human Resources
Julie Lynch
(508) 820-8162

Executive Vice President, Strategic Programs
Ronald L. Milton
(508) 820-8661

Vice President/Group Publisher Computerworld.com
Gregg Pinsky
(508) 271-8013

Executive Vice President/COO
Matthew C. Smith
(508) 820-8102

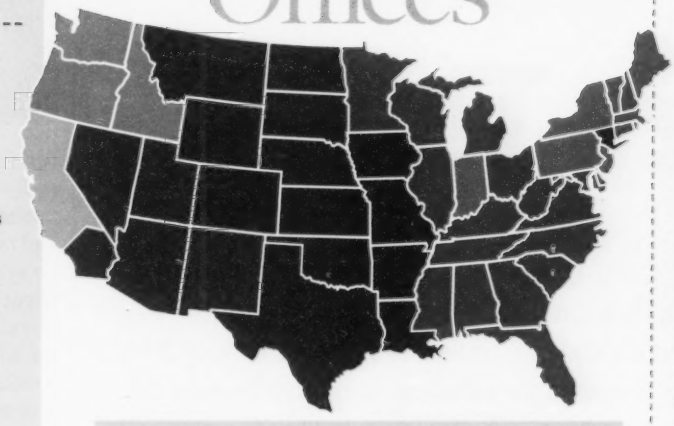
IDG

International Data Group Chairman of the Board
Patrick J. McGovern

CEO, IDG Communications
Bob Carrigan

Computerworld is a business unit of IDG, the world's leading technology media, research and events company. IDG publishes more than 300 magazines and newspapers and offers online users the largest network of technology-specific sites around the world through IDG.net (*www.idg.net*), which comprises more than 330 targeted Web sites in 80 countries. IDG is also a leading producer of 168 computer-related events worldwide, and IDG's research company, IDC, provides global market intelligence and advice through 51 offices in 43 countries. Company information is available at *www.idg.com*.

Sales Offices



President/CEO
Matthew J. Sweeney (508) 271-7100
Fax (508) 270-3882

Vice President/Publisher, Integrated Programs & Events
John Amato (508) 820-8279
Fax (508) 626-8524

Senior Sales Operations Manager
Dawn Cora (508) 820-8133

■ NORTHWESTERN STATES
■ BAY AREA
■ SOUTHWESTERN STATES
■ CENTRAL STATES
Vice President/ Associate Publisher of Custom Programs
Bill Hanck (949) 442-4006

Mailing Address
19200 Von Karman Avenue
Suite 360, Irvine, CA 92612
Fax (949) 476-8724

Account Director
Lauren Guerra (415) 978-3306

Senior Sales Associate, Integrated Programs
Chris Da Rosa (415) 978-3304

Mailing Address
501 Second Street, Suite 114
San Francisco, CA 94107
Fax (415) 543-8010

Senior Sales Associate, Integrated Programs
Emmie Hung (415) 978-3308

■ SOUTHEASTERN STATES
Vice President, Integrated Programs
Lisa Ladle-Wallace (904) 284-4972

Mailing Address
5242 River Park Villas Drive
St. Augustine, FL 32092
Fax (800) 779-8622

Senior Sales Associate, Integrated Programs
Jess Roman (508) 271-7108

Mailing Address
P.O. Box 9171, 1 Speen Street
Framingham, MA 01701
Fax (508) 270-3882

■ NEW ENGLAND STATES
Vice President, Integrated Programs
Deborah Crimmings (508) 271-7110

Senior Sales Associate, Integrated Programs
Jess Roman (508) 271-7108

Mailing Address
P.O. Box 9171, 1 Speen Street
Framingham, MA 01701
Fax (508) 270-3882

■ METRO NEW YORK
■ EASTERN CENTRAL STATES/INDIANA
Vice President, Integrated Programs
Peter Mayer (201) 634-2324

Senior Sales Associate, Integrated Programs
John Radzniak (201) 634-2323

Mailing Address
650 From Road, Suite 225
Paramus, NJ 07652
Fax (201) 634-9289

CIRCULATION/DISTRIBUTION
Vice President
Debbie Winders (508) 820-8193

Circulation Manager
Diana Turco (508) 820-8167

Distribution and Postal Affairs
Michelle Fuller (508) 628-4757

PRODUCTION
Vice President, Production
Carolyn Medeiros

Production Manager
Kim Pennett

Print Display Advertising
(508) 820-8232
Fax (508) 879-0446

STRATEGIC PROGRAMS AND EVENTS
Vice President, Business Development John Vulopas

Vice President, Strategic Programs & Events Ann Harris

Vice President, Event Marketing and Conference Programs Derek Hulitzky

Senior Director, Event Management
Michael Meleedy

Executive Programs Specialist
Executive Assistant Kelly McGill
Fax (508) 626-8524

ONLINE ADVERTISING
Vice President/Associate Publisher
Sean Weglage (415) 978-3314
Fax (415) 543-8010

Online Sales Directors
James Kalbach
(610) 971-1588

Jennell Hicks
(415) 978-3309
Fax (415) 543-8010

Online Sales Manager
Matthew Wintringham
(508) 820-8218
Fax (508) 270-3882

Account Services Director
Bill Rigby (508) 820-8111
Fax (508) 270-3882

Online Sales Assistant
Joan Olson (508) 270-7112
Fax (508) 270-3882

IT CAREERS
Senior Sales Operations Manager
Dawn Cora (508) 820-8133
Fax (508) 626-8524

LIST RENTAL
Postal and E-mail
Rich Green (508) 370-0832
rgreen@idglist.com

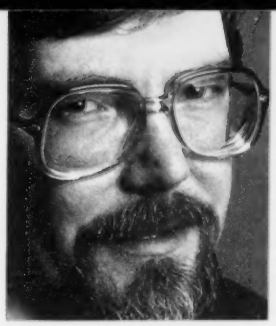
Mailing Address
IDG List Services, P.O. Box 9151
Framingham, MA 01701-9151
Fax (508) 370-0020

Customer Service
(888) 559-7327 toll free
Local or outside U.S.
(847) 559-1573
E-mail: cw@omeda.com

■ FRANKLY SPEAKING

Frank Hayes

Crazy Time



TERRY CHILDS is in the news again. Remember Childs, that lone-wolf network administrator who worked for the city of San Francisco? In July 2008, he was arrested for refusing to tell his bosses the passwords to the city's high-speed network. He's been in jail ever since because he hasn't made his $5 million bail.

Now he's asking the city to pay $3 million for canning him.

Crazy, huh?

Specifically, Childs filed a claim for "wrongful suspension without pay and wrongful arrest [and] violation of civil rights," according to the claim form dated Jan. 8. That $3 million breaks down as $1 million for economic damages — most likely lost pay and benefits — plus $1 million for emotional distress and $500,000 each for attorney's fees and unspecified "special damages."

Remember, this is after Childs allegedly changed the network's passwords so only he knew them, installed modems to gain outside access to the network, configured routers so they could be controlled only from obscure locations, harassed an auditor, threatened his boss, lied to investigators about knowing the passwords and finally turned the passwords over to San Francisco's mayor.

Yes, it all sounds wacko. But actually, this wrongful-suspension claim isn't a surprise. Childs was suspended on July 9; he had six months to file a claim, which was necessary if he ever wanted to sue the city. His claim was turned down on Jan. 23, and now he has another six months to file a lawsuit. Makes sense now, right?

Meanwhile, Childs will be in court next week to be arraigned on the criminal charges against him: tampering with a computer network, denying other authorized users access to the network and causing more than $200,000 in losses. If he squeaks through the criminal case, he'll have a shot — albeit a very long one — at getting his $3 million.

■ Is there a Terry Childs in your IT shop? Let's hope not. But it doesn't take extreme behavior to create an epic failure.

As for the rest of us — well, we've got troubles of our own, don't we? We're dealing with budget cuts, layoffs, longer hours and shorter tempers. Why should we care about some net admin who went over the edge?

But maybe that's *exactly* what we should care about.

Six months ago, I wrote that the Terry Childs fiasco carried a lesson for everyone in IT shops: As the only person with control of the city's network backbone, Childs was a single point of failure. That made him a reliability risk — one that, uncorrected, eventually created a huge problem.

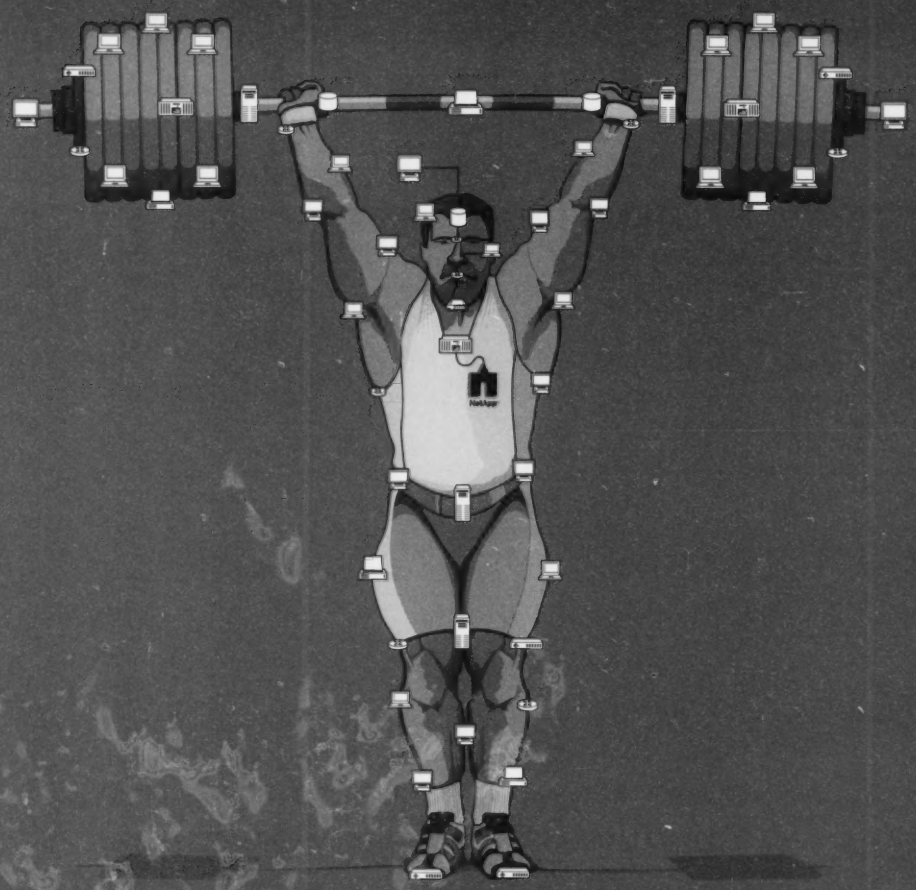
Now it's worse. Today, deep in a recession, we're *all* at risk, from the CIO down to the lowliest help desk tech. We're short-staffed, overworked and under pressure. More and more, we depend on every person in the department. We've got no cushion, no safety net. Each of us could become a reliability problem — and we're too cash-strapped to eliminate every single point of failure.

Is there a Terry Childs in your IT shop? Let's hope not. But it doesn't take extreme behavior to create an epic failure. It doesn't even take a little craziness. Under this pressure, we can get sloppy, cut corners and miss warning signs that eventually cost us in a big way — and that's when it comes to both systems *and* people.

Don't let it happen. Make sure everyone in your shop takes a little extra time and care with the hardware *and* the techs, the networks *and* the admins. Reinforce your procedures, your fail-over plans and your teams — and especially the people who you *really* can't afford to have fail.

Because in crazy times like these, that may be the only safety net you've got. ■

Frank Hayes *is* Computerworld's *senior news columnist. Contact him at frank_hayes@computerworld.com.*



With NetApp® at the heart of your business, you can

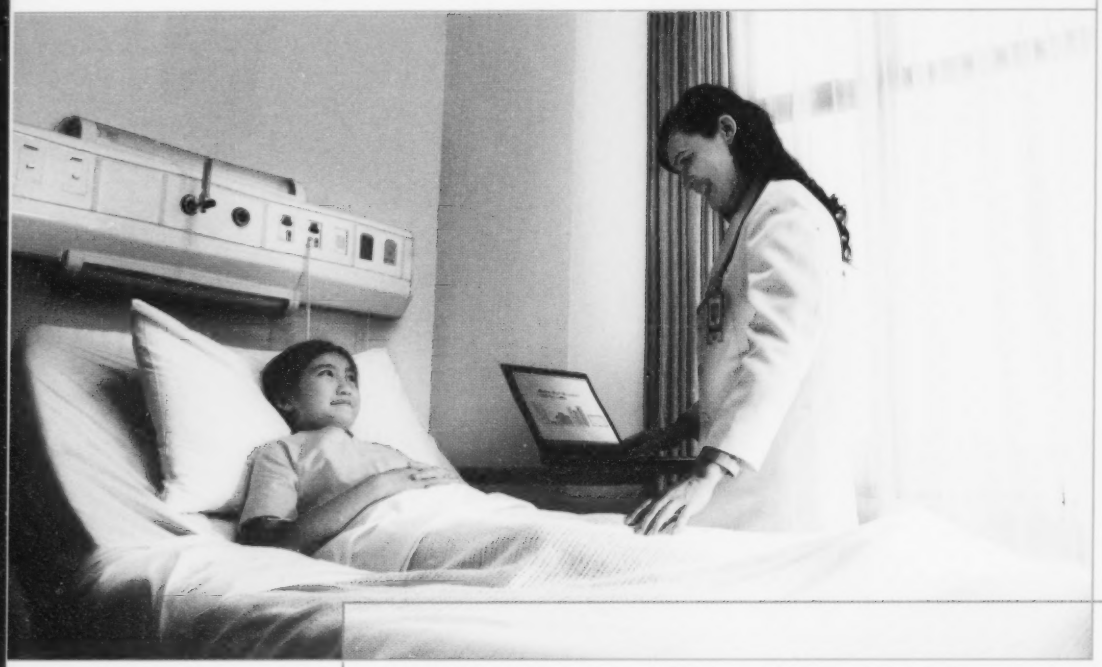
EFFORTLESSLY HOLD YOUR DATA

at a fraction of the cost and footprint.

Imagine storage and data management solutions smart enough to support the data you need, and not a lot of dead weight. It's possible when you partner with NetApp. Our industry-leading solutions use deduplication and other space-saving technologies to help you store data efficiently and reduce your footprint by 50% or more. So you can manage exponential growth while minimizing your storage investment—all with the support of a team that will exceed your expectations. See how we can help your business go further, faster. Find out how you can use 50% less storage, guaranteed,* at netapp.com/efficiency.

NetApp™
Go further, faster

© 2009 NetApp. All rights reserved. Specifications are subject to change without notice. NetApp, the NetApp logo, and Go further, faster are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. *This guarantee and related Program is limited to the terms set forth in the Program Guide and Acknowledgement For 50% Virtualization Guarantee Program document, applicable only to prospective orders placed after the Program effective date and is dependent upon your compliance with the terms and conditions set forth in this document and any of the instruction sets and specifications set forth in the referenced documents. NetApp's sole and exclusive liability and your sole and exclusive remedy associated with the terms of this guarantee and related Program is the provision by NetApp of the additional storage capacity as set forth in this guarantee and related Program.



NEC's advanced communications solutions put you in charge when it matters most.

Finally, a communications solution capable of providing up-to-date patient information whenever and wherever it is needed.

NEC's Unified Communications provide a dynamic and realistic connection among individuals, devices, applications, and data. Based on a combination of innovative technologies and advanced solutions, its mobility and flexibility enables people to experience greater efficiency and productivity – in any industry.

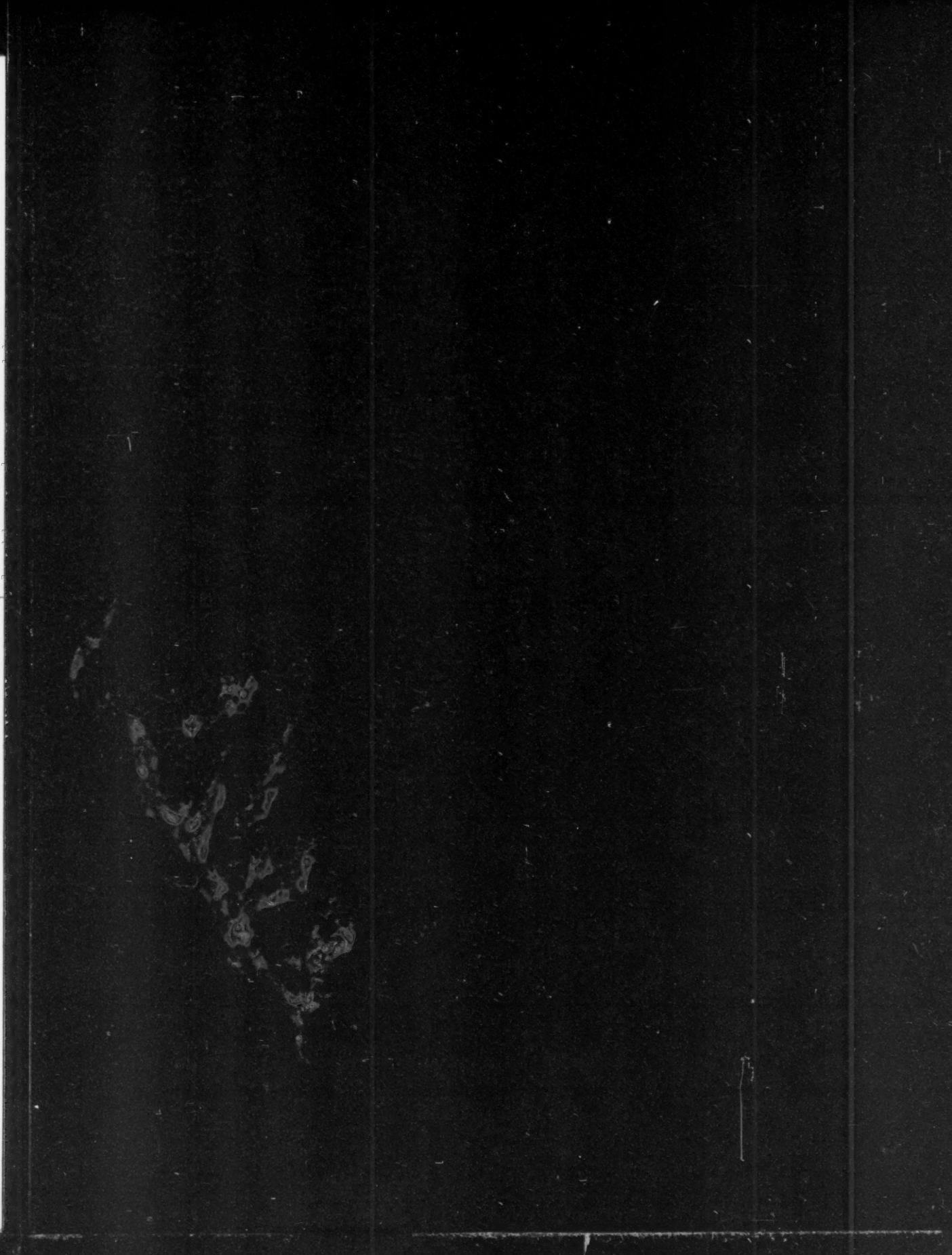
Integrated IT and networking solutions like these have made NEC a world leader, and your reliable business partner.

Regardless of the communications solution your business demands, you are assured of one thing. NEC empowers you through innovation.

www.necus.com/uc

IT SERVICES AND SOFTWARE NETWORKING AND COMPUTING SEMICONDUCTORS IMAGING AND DISPLAYS

©NEC Corporation 2008.
NEC and the NEC logo are registered trademarks of NEC Corporation.
Empowered by Innovation is a trademark of NEC Corporation.

Empowered by Innovation

NEC